QUANTIFIZIERUNG OPERATIONELLER TECHNOLOGIERISIKEN BEI KREDITINSTITUTEN

Eine Ontologie-zentrierte Vorgehensweise im Spannungsfeld bankinterner und aufsichtsrechtlicher Sichtweise

Inauguraldissertation
zur Erlangung des akademischen Grades
eines Doktors der Wirtschaftswissenschaften
der Universität Mannheim

vorgelegt von

Diplom-Wirtschaftsinformatiker
Christian Cuske

aus Wuppertal

im September 2006

Vorwort

Die vorliegende Arbeit ist die veröffentlichte Fassung meiner Dissertation im Bereich der Quantifizierung operationeller Technologierisiken im Umfeld von Kreditinstituten. Sie verbindet wesentliche Aspekte der aktuellen Diskussion um IT-Governance und Basel II mit Anregungen aus meiner Projekttätigkeit. Die Dissertation entstand während meiner Zeit als externer Doktorand am Lehrstuhl für Wirtschaftsinformatik III der Universität Mannheim.

Mein erster Dank gilt so meinem Doktorvater Herrn Prof. Dr. Martin Schader, der mir die Möglichkeit gegeben hat, mein Promotionsvorhaben an seinem Lehrstuhl in die Tat umzusetzen. Hier habe ich in einer konstruktiven Arbeitsumgebung wissenschaftliche Hintergründe und Methoden mit meinen beruflichen Erfahrungen zusammenbringen können. Ebenso möchte ich mich bei Herrn Prof. Dr. Dr. h.c. Wolfgang Bühler für wertvolle Anregungen sowie die Übernahme des Korreferats bedanken. Herrn Prof. Dr. Roland Vaubel danke ich für die Teilnahme an meiner mündlichen Prüfung.

Ein besonderer Dank geht auch an alle Lehrstuhlkollegen, die mich von Anfang an als Teil des Teams aufgenommen haben. Dies gilt insbesondere für Tilo Dickopp, Dr. Axel Korthaus und Stefan Seedorf, mit denen ich an mehreren interessanten Projekten zusammengearbeitet habe. Ferner möchte ich Dr. Markus Aleksy für die gute Unterstützung und Dr. Ralf Gitzel für sehr wertvolle Diskussionen während meiner Zeit am Lehrstuhl danken.

Meinen Eltern Eva und Horst-Peter Cuske danke ich ganz besonders dafür, dass sie stets Anteil genommen und mir meine Promotion überhaupt erst ermöglicht haben. Meiner Frau Christine schulde ich den meisten Dank, da sie mir über die gesamte Zeit hinweg in ganz besonderer Weise den Rücken freigehalten hat.

Mannheim im Mai 2007 Christian Cuske

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AktG	Aktiengesetz
AMA	Fortgeschrittener Messansatz (Advanced Measurement Approach)
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
Basel I	Internationale Konvergenz der Eigenkapitalmessung und Eigenkapitalanforderungen
Basel II	Internationale Konvergenz der Eigenkapitalmessung und der Eigenkapitalanforderungen - Überarbeitete Rahmenvereinbarung
BBA	British Bankers' Association
BCBS	Basel Committee on Banking Supervision
BIS	Bank for International Settlement
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAD III	Capital Adequacy Directive III
CEIOPS	Committee of European Insurance and Occupational Pensions Supervisors
CVaR	Conditional Value at Risk
COBIT	Control Objectives for Information and related Technology
DAML	DARPA Agent Markup Language
DARPA	Defense Advanced Research Projects Agency
DL	Description Logic
EUR	Euro
FAIT	Fachausschuss für Informationstechnologie des IDW
GO30	Group of 30
GPD	Generalisierte Pareto-Verteilung (Generalized Pareto-Distribution)

HGB	Handelsgesetzbuch
IAS	International Accounting Standards
IDW	Institut der Wirtschaftsprüfer
IFRS	International Financial Reporting Standards
ISDA	International Swaps and Derivatives Association
IT	Informationstechnologie
ITGI	IT Governance Institute
ITGS	IT-Grundschutz
JNI	Java Native Interface
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
KWG	Kreditwesengesetz
LDCE	Loss Data Collection Exercise
LPM	Lower Partial Moments
MaRisk	Mindestanforderungen an das Risikomanagement
OIL	Ontology Inference Layer
OTC	Over the Counter
OWL	Web Ontology Language
PS	Prüfungsstandard des IDW
RDF	Resource Description Framework
RDFS	RDF Schema
RMA	Risk Management Association
RMG	Risk Management Group
RS	Rechnungslegungsstandard
SLA	Service Level Agreements
Solvency II	Entwurf einer Richtlinie zur Solvabilität bei Versicherungen
SolvV	Solvabilitätsverordnung
SPARQL	SPARQL Protocol and RDF Query Language
Tz	Textziffer

UML	Unified Modeling Language
URI	Unified Resource Identifier
USD	US amerikanische Dollar
VaR	Value at Risk
W3C	World Wide Web Consortium
XML	Extensible Markup Language

Kapitel 1
Herausforderung Technologierisiken

Internationale Kreditinstitute bewegen sich in einem Umfeld, das durch stetige Veränderungen, eine umfassende Regulierung sowie einen zunehmenden Kostendruck geprägt ist. Nicht zuletzt daher kann im europäischen und auch deutschen Bankensektor eine verstärkte Konsolidierungsbewegung wahrgenommen werden. In diesem Zusammenhang stehen Kreditinstitute kontinuierlich vor der Aufgabe, die strategische Ausrichtung zu überdenken sowie die internen Strukturen an neue Gegebenheiten anzupassen. Eine zentrale Rolle spielt im modernen Bankenumfeld hierbei die Informationstechnologie (IT), die der Dynamik jeglicher Veränderung kontinuierlich folgen muss. Diese Überlegung stellt die Grundlage für die in den folgenden Abschnitten dargestellte Ausgangslage, Zielsetzung und Gliederung dieser Arbeit dar.

1.1 Rechtfertigung der Themenstellung

Die Bedeutung der Informationstechnologie für Kreditinstitute ist in den letzten Jahren beständig gestiegen. Als einer der exogenen Gründe kann die vermehrte Forderung nach IT-getriebenen Bankdienstleistungen wie beispielsweise internetbasiertem Privatkundengeschäft und elektronischem Handel gesehen werden. Des Weiteren führt der starke Kostendruck zu einem höheren Grad der Automatisierung interner Prozesse durch den Einsatz von Informationstechnologie. Hierbei kommen bei Kreditinstituten vermehrt standardisierte Anwendungssysteme, wie SAP for Banking, zum Einsatz. Eine weitere wesentliche Motivation für technologische Veränderungen bei Banken ist in der Weiterentwicklung der regulatorischen Anforderungen zu sehen. Beispielsweise führt die Umstellung auf internationale Rechnungslegungsstandards (IAS/IFRS) besonders im Rechnungswesen zu gravierenden Modifikationen der Systemlandschaft. Ein zusätzlicher wichtiger Aspekt ergibt sich aus den im internationalen Bankensektor stattfindenden Fusionen und Übernahmen. Hier sind für den europäischen Raum exemplarisch die Übernahme der HypoVereinsbank durch die italienische UniCredit sowie die Fusion großer Teile der genossenschaftlichen

Zentralbanken zur DZ BANK zu nennen. Dabei hat sich gezeigt, dass die Integration bestehender Anwendungssysteme in eine gemeinsame IT-Landschaft stets eine besondere Herausforderung darstellt.

Direkte Konsequenz der wachsenden Bedeutung von Informationstechnologie bei Kreditinstituten ist die Zunahme der durch ihren Einsatz entstehenden Risiken (vgl. BCBS 2003b, S.1f.). Beispielsweise stellen Systemausfälle durch Computerviren oder unerlaubte Systemzugriffe eine Bedrohung für das Geschäft von Banken dar. Werden verstärkt zentrale Geschäftsprozesse durch Anwendungssysteme unterstützt, entstehen zwangsläufig direkte Abhängigkeiten. So können durch einen Systemausfall entscheidende Geschäftsabläufe innerhalb der Bank gestört werden. Ferner liegt in der Einführung neuer Anwendungssysteme oder der fusionsbedingten Migration verschiedener Architekturen ein großes Fehlerpotential. Aktuelle Beispiele zeigen, dass solche Risiken zu bestandsgefährdenden Verlusten bei Banken führen können (vgl. BCBS 2004, S.67).

Hieraus ergibt sich, dass das Management der Technologierisiken integraler Bestandteil einer Gesamtbanksteuerung sein muss. Dies sollte im Rahmen der IT-Governance erfolgen:

„The overall objective of IT governance [...] is to understand the issues and the strategic importance of IT, so that the enterprise can sustain its operations and implement the strategies required to extend its activities into the future. IT governance aims at ensuring that expectations for IT are met and IT risks are mitigated.“ (IT Governance Institute 2003, S.7)

Der IT-Governance obliegt die Verantwortung, das Verhältnis von Rendite und Risiko im Zusammenhang mit der eingesetzten Informationstechnologie zu steuern. In diesem Sinne begreift die IT-Governance die eingegangenen Technologierisiken als entscheidende ökonomische Größe im Kontext der gesamten Unternehmenssteuerung. Das IT Governance Institute nennt fünf wesentliche Themengebiete der IT-Governance: den realisierten Wertbeitrag der IT, das Management der Technologierisiken, die strategische Ausrichtung der gesamten IT, das Management der genutzten Ressourcen und die letztendliche Erfolgskontrolle (vgl. IT Governance Institute 2003, S.19).

Zusätzlich zu dieser unternehmensinternen Argumentation erzwingen auch veränderte aufsichtsrechtliche Anforderungen, Technologierisiken in das bankweite Risikomanagement zu integrieren. Ab 2007/2008 ist die Anwendung der „überarbeiteten internationalen Rahmenvereinbarung zur Konvergenz der Eigenkapitalmessung und Eigenkapitalanforderungen“ (kurz Basel II) verpflichtend. Im Einzelnen ist jeweils die entsprechende europäische beziehungsweise nationale Umsetzung maßgeblich. Allgemein sind nach Basel II auch operatio-

nelle Risiken aus den Geschäftsabläufen der Bank erstmalig mit aufsichtsrechtlichem Kapital zu unterlegen. Das betrifft somit direkt auch die Technologierisiken, da diese Bestandteil allgemeiner operationeller Risiken sind.

Die regulatorische Berücksichtigung operationeller Risiken basiert auf drei Säulen. Erstens muss das Risikopotential quantitativ erfasst und ausreichend abgesichert werden. Zweitens muss der bankinterne Risikomanagementprozess um qualitative Aspekte ergänzt und überprüfbar gestaltet werden. Im dritten Schritt muss das Risikoprofil anspruchsberechtigten Dritten offengelegt werden.

Insbesondere im Bereich der Quantifizierung operationeller Risiken ist die Entwicklung zuverlässiger Methoden jedoch noch nicht abgeschlossen. Grund ist das im Vergleich zu Markt- oder Kreditrisiken nicht klar umrissene Verständnis operationeller Risiken. In der folgenden Tabelle 1.1 wird dieser Unterschied insbesondere im Hinblick auf Umfang, Ursache und Auswirkung deutlich.

	Marktrisiken	**Kreditrisiken**	**Operationelle Risiken**
Reguliert seit:	Basel I (1996)	Basel I (1988)	Basel II (2004)
Umfang:	Positionen in Wertpapieren oder Derivaten	Vergebene Kredite, in Teilen Ausfallrisiken im Handel	Sämtliche für den Bankbetrieb benötigten Ressourcen
Ursache:	Änderungen in Marktpreisen, Zinssätzen	Verschlechterung der Bonität, Ausfälle eines Kreditnehmers	Ausfälle benötigter Ressourcen
Auswirkung:	Abschreibungen, Veränderung des Ergebnisses	Abschreibungen, Zuführung zur Risikovorsorge	Vielzahl möglicher finanzieller Effekte

Tabelle 1.1: Wichtige Bankrisiken

Die Risikoquantifizierung jedoch ist ein entscheidender Aspekt im Management der operationellen und damit auch der Technologierisiken. Sie dient sowohl der Ermittlung bankinterner Steuerungsgrößen als auch der Bestimmung aufsichtsrechtlich geforderter Eigenkapitalreserven. Wesentliche Begründung für die aufsichtsrechtliche Forderung nach Unterlegung mit Eigenkapital ist die Verhinderung von Bankenkrisen. Das bankinterne Risikomanagement hingegen zielt auf eine risikoadjustierte Steuerung der Abläufe ab. Aufgrund der unterschiedlichen Zielsetzung betriebswirtschaftlicher und aufsichtsrechtlicher Herangehensweisen muss die Frage gestellt werden, ob für Technologierisiken ein beide Sichtweisen integrierender Ansatz möglich ist. Eine häufig genannte Kri-

tik unterstreicht die Notwendigkeit: *„[Operational] risk is now increasingly viewed as yet another compliance exercise“* (Jeffery 2005, S.91). Es erscheint somit erforderlich, die Entwicklung einer Vorgehensweise zur Quantifizierung von Technologierisiken zu untersuchen, welche zugleich unternehmerischen und aufsichtsrechtlichen Anforderungen genügt.

1.2 Zielsetzung der Arbeit

Ziel der vorliegenden Arbeit ist es deshalb, unter der Berücksichtigung regulatorischer Rahmenbedingungen eine auf die Belange der Banksteuerung ausgerichtete Vorgehensweise zur Quantifizierung von Technologierisiken zu entwickeln. Diese muss im Kern auf einem ausgeprägten Verständnis dieser noch unscharfen und nicht ausreichend abgegrenzten Risikokategorie basieren. Denn nur ein wirkliches Verständnis der Technologierisiken macht ein unternehmerisch wirkungsvolles Management erst möglich. Diese Forderung ist in allgemeiner Form im qualitativen Teil der Basler Rahmenvereinbarung enthalten:

„Bank management is responsible for understanding the nature and level of risk being taken by the bank and how this risk relates to adequate capital levels.“ (Basel II, Tz.728)

Auch das IT Governance Institute unterstreicht die besondere Bedeutung des Verständnisses der Technologie-bezogenen Risiken:

„Often, the most damaging IT risks are those that are not well understood.“
(IT Governance Institute 2003, S.27)

Diese noch abstrakte Forderung wird für die vorliegende Arbeit in Form zweier zentraler Ziele schrittweise konkretisiert:

Das erste Ziel ist es, ein Modell operationeller Technologierisiken zu entwickeln, welches ein bankweites und explizites Risikoverständnis ermöglicht.

(1a) Eine wesentliche Voraussetzung für das Verständnis operationeller Technologierisiken ist ein klar abgegrenzter und prägnanter Risikobegriff. Dieser muss sowohl Konzepte der IT-Governance beinhalten als auch regulatorische Anforderungen berücksichtigen.

(1b) Dieses Risikoverständnis muss in einem weiteren Schritt um bankspezifische Besonderheiten und Strukturen erweitert werden. In diesem Sinne muss das organisatorische Wissen über risikorelevante Ursache-Wirkung-Beziehungen in das Modell der Technologierisiken einfließen.

(1c) Da sowohl die verwendeten Begriffe als auch die zugrunde liegenden Strukturen einem ständigen Wandel unterliegen, muss das Modell flexibel genug sein, auf solche Veränderungen reagieren zu können. Konkret muss es möglich sein, das spezifizierte Verständnis beziehungsweise Wissen in einem kontinuierlichen Prozess anzupassen.

Zusammengefasst kann das erste Ziel – Verständnis von Technologierisiken – in drei Teilziele untergliedert werden: Schaffung einer klaren unternehmerischen und aufsichtsrechtlich zulässigen Begriffsabgrenzung (a), Berücksichtigung des organisatorischen Wissens und der Zusammenhänge der Bank (b) sowie Berücksichtigung von Veränderungen der Begriffe und Strukturen (c).

In der Literatur existiert bisher kein geeigneter Ansatz, der allen diesen Anforderungen genügt. Die Entwicklung eines geeigneten Modells operationeller Technologierisiken ist somit erster wichtiger Aspekt dieser Arbeit.

Das zweite Ziel ist es, eine belastbare Methode zur Quantifizierung von Technologierisiken zu entwickeln, welche auf dem bankweiten und expliziten Risikoverständnis basiert.

(2a) Eine Voraussetzung der Quantifizierung ist die möglichst genaue und belastbare Ermittlung des finanziellen Risikopotentials. Entscheidend ist hierzu eine breite und objektive Datenbasis.

(2b) Entscheidend für die Güte der Quantifizierung ist der inhärente Zusammenhang zwischen der ermittelten Kennzahl und der tatsächlichen Risikosituation. Veränderungen in der Risikosituation müssen durch ein sensitives Risikomaß unmittelbar und sachgemäß reflektiert werden.

Zusammenfassend kann das zweite Ziel – Quantifizierung von Technologierisiken – unter den Begriffen Objektivität der Daten (a) und Risikosensitivität (b) subsumiert werden. Die Quantifizierung muss zudem möglichst eng mit dem formalen Verständnis der Technologierisiken verknüpft sein. Zur Risikomessung existieren diverse Methoden, die in unterschiedlicher Weise die Aspekte Verständnis und Quantifizierung kombinieren. Bisher steht jedoch keine Methode für Technologierisiken zur Verfügung, die beiden Zielen ausreichend Rechnung trägt. Das liegt hauptsächlich darin begründet, dass die zentrale Triebfeder der Entwicklung bisher mehr die Erfüllung regulatorischer Anforderungen gemäß Basel II und nicht die Umsetzung einer bankweiten IT-Governance ist.

Eine auch bankinternen Ansprüchen genügende Methode zur Quantifizierung von Technologierisiken wird zwangsläufig über die Umsetzung der ersten Säule von Basel II hinausgehen. Da hiermit auch erhöhte Kosten verbunden sein werden, ist diese Vorgehensweise primär für stark risikobehaftete Szenarien relevant. Der zentrale Beitrag der Arbeit ist es, im Spannungsfeld zwischen bankinterner IT-Governance und Basel II eine verständnisorientierte und ursachenbezogene Vorgehensweise zur Quantifizierung operationeller Technologierisiken zu entwickeln. Diese muss Konzepte aus der IT-Governance sowie aus Basel II einbinden und ein aus Sicht der Bank sinnvolles Technologierisiko-Management ermöglichen.

1.3 Übersicht über die Vorgehensweise

Die vorliegende Arbeit beschreibt nun die Umsetzung einer mit den beiden zentralen Zielen konformen Vorgehensweise zur Entscheidungsunterstützung im Risikomanagement bei Kreditinstituten (vgl. Abbildung 1.1). Im Anschluss an die Darstellung grundlegender Aspekte des quantitativen Risikomanagements in Kapitel 2 wird ein Begriffsverständnis aus der Literatur abgeleitet und darauf aufbauend eine Methode zu Quantifizierung entwickelt. Diese wird prototypisch implementiert und abschließend in einem Fallbeispiel evaluiert.

Die Verwendung formaler Ontologien stellt einen durchgehenden Aspekt sowohl in der konzeptionellen als auch der methodischen sowie der technischen Umsetzung dieser Arbeit dar. Das Konzept formaler Ontologien wird erstmals in der Begriffsbildung im Rahmen von Kapitel 3 eingesetzt, um die verwendete Terminologie explizit festzulegen. Durch die Entwicklung einer Ontologie operationeller Technologierisiken werden die unterschiedlichen existierenden Konzepte, Eigenschaften und Strukturen aus der Literatur zu IT-Governance und Basel II zusammengeführt.

Ein weiteres Ziel ist es, die Quantifizierung eng mit dem entwickelten Modell operationeller Technologierisiken zu verknüpfen. In Kapitel 4 werden zunächst existierende Methoden auf ihre Tauglichkeit hierfür untersucht. Auf Grundlage der dabei identifizierten Schwächen wird eine Ontologie-zentrierte Vorgehensweise vorgeschlagen, die existierende simulationsgestützte Ansätze erweitert und mit der Technologierisiko-Ontologie verbindet. Die hier entwickelte Simulation stellt in diesem Sinne ein neues Werkzeug zur Entscheidungsunterstützung dar. Sie wird dabei jedoch nicht zur Prüfung einer aufgestellten Theorie oder zur Analyse bestimmter Implikationen auf ein theoretisches Modell herangezogen (vgl. Weber 2004, S.183ff.).

Um die technische Machbarkeit der theoretisch beschriebenen Konzepte zu demonstrieren, wird in dieser Arbeit der Ansatz des Prototypenbaus verfolgt (vgl. Becker et al. 2004, S.347f.). In Kapitel 5 wird daher eine mögliche Implementierung der Ontologie-zentrierten Vorgehensweise beschrieben. Hier wird insbesondere darauf eingegangen, wie Eigenschaften von Ontologien und deren Repräsentationssprachen genutzt werden können, um den ganzheitlichen Ansatz auch technisch zu realisieren.

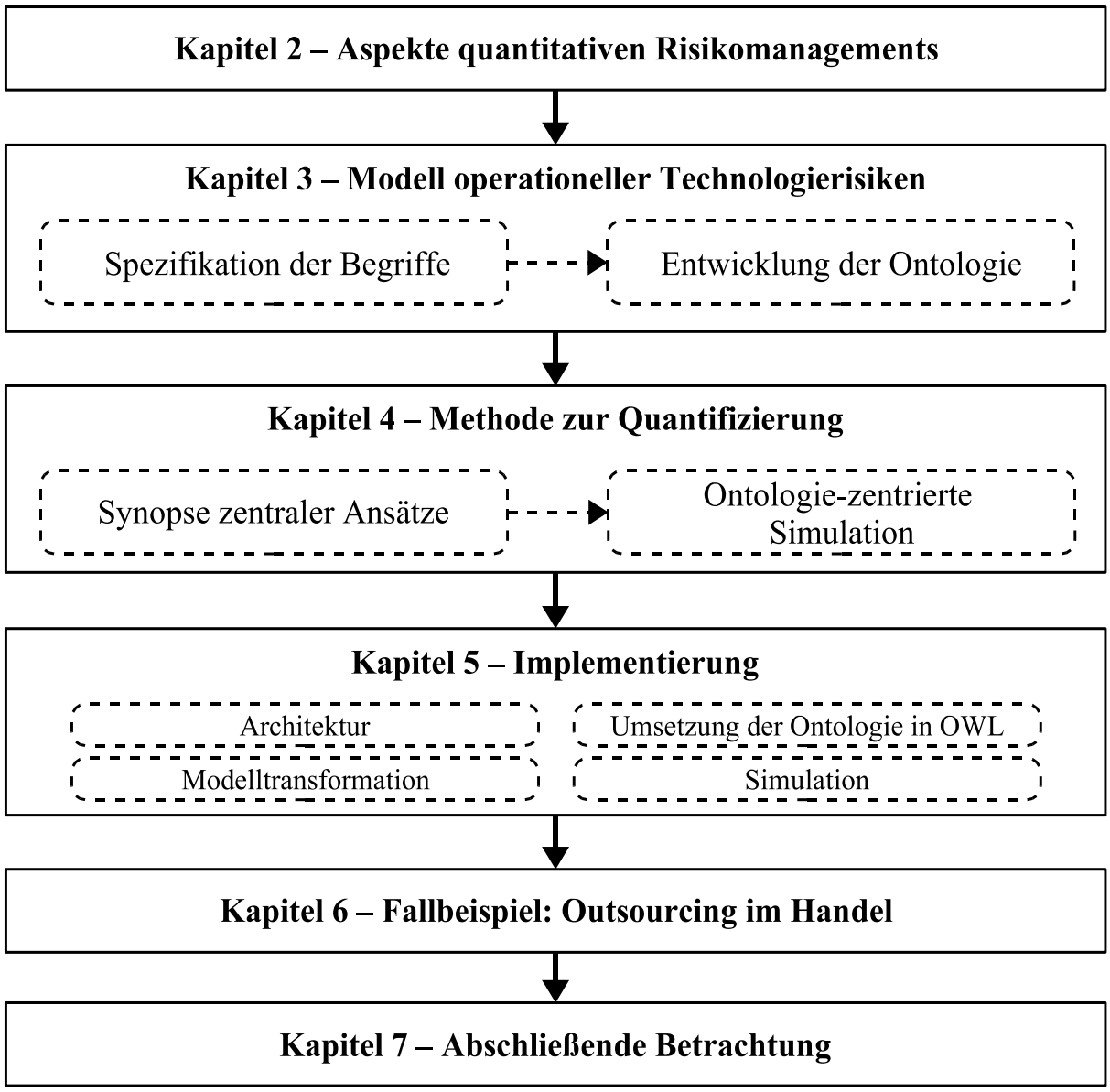

Abbildung 1.1: Übersicht der Gliederung

Die vorgeschlagene Ontologie-zentrierte Vorgehensweise wird in Kapitel 4 abstrakt und allgemeingültig definiert. Zum besseren Verständnis wird deshalb in Kapitel 6 ein in die deutsche Bankenregulierung eingebettetes Fallbeispiel vorgestellt. Dieses beschreibt die Risikoquantifizierung im Handel einer idealtypischen Großbank unter dem Einfluss eines Outsourcing-Szenarios. Hierüber erfolgt indirekt ein „proof of concept“ der vorgeschlagenen Ontologie-zentrierten Vorgehensweise.

In Kapitel 7 werden das Technologierisiko-Modell sowie die Ontologie-zentrierte Simulation einer kritischen Würdigung unterzogen. Abschließend wird ein Ausblick auf weitere Entwicklungsmöglichkeiten wie den Einsatz von Ontologien innerhalb des gesamten Risikomanagementprozesses oder den Transfer in die Versicherungswirtschaft gegeben.

Kapitel 2
Aspekte quantitativen Risikomanagements

Kreditinstitute stellen einen wichtigen Bestandteil heutiger Wirtschaftsräume dar. Daher ist ein *„[...] funktionstüchtiges Bankwesen [...] für die Leistungsfähigkeit einer Volkswirtschaft sehr wichtig. Denn nur ein stabiles Finanzsystem kann seine gesamtwirtschaftliche Funktion – die kostengünstige Transformation und Bereitstellung finanzieller Mittel – erfüllen“* (BaFin 2006). Einen entscheidenden Beitrag zur Stabilität jedes einzelnen Kreditinstituts stellt das Management der eingegangenen Risiken dar. Nur so kann die Wahrscheinlichkeit erkannt, analysiert und minimiert werden, dass ein Kreditinstitut aufgrund ungünstiger Marktbewegungen, hoher Kreditausfälle oder schwerer Verfahrensfehler im Fortbestand gefährdet ist. Ein zentraler Bestandteil des Risikomanagements ist die Quantifizierung der Risiken, also die Abschätzung möglicher finanzieller Verluste. Die Ermittlung des Risikopotentials ist sowohl Basis einer risikoorientierten Gesamtbanksteuerung als auch einer aufsichtsrechtlichen Forderung nach ausreichenden Eigenkapitalreserven im Verlustfall. Ziel dieses Kapitels ist es, Grundlagen für die Entwicklung einer umfassenden Vorgehensweise zur Quantifizierung operationeller Technologierisiken zu legen. Hierzu werden zuerst Bestandteile eines quantitativen Risikoverständnisses allgemeiner Geschäfts- und operationeller Risiken erläutert, um daraus die für diese Arbeit relevanten Definitionen abzuleiten. Im Anschluss wird die besondere Bedeutung des Risikomanagements in Kreditinstituten aufgezeigt. Abschließend stehen die für eine technische Umsetzung benötigten Grundlagen der Ontologiezentrierten Simulation im Vordergrund.

2.1 Abgrenzung des Risikoverständnisses

Für die Entwicklung eines quantitativen Verständnisses allgemeiner Geschäfts- und operationeller Risiken werden zunächst gängige Ansätze aus der Literatur zur Begriffsbildung aufgezeigt und mit dem mathematischen Wahrscheinlichkeitsbegriff verbunden. Auf dieser Basis werden die verteilungsbasierten Risikomaße analysiert, die in dieser Arbeit zur Quantifizierung verwendet werden.

2.1.1 Allgemeine Geschäftsrisiken

Der Begriff des Risikos wird in der betriebswirtschaftlichen Literatur nicht durchgängig eindeutig oder trennscharf definiert (vgl. Farny 1979, S.13; Braun 1984, S.22; Baetge und Schulze 1998, S.938). Jedoch wird in weiten Teilen davon ausgegangen, dass zumindest eine gemeinsame Basis der verwendeten Begriffe existiert (vgl. Kupsch 1973, S.26; Braun 1984, S.22). Im Folgenden werden gängige ökonomische Ansätze (siehe Neubeck 2003) sowie ergänzend eine mathematische Interpretation des Risikobegriffs dargestellt, um daraus eine für diese Arbeit geeignete Definition abzuleiten:

- Extensives Risikoverständnis,
- Ursachenbezogener Risikobegriff,
- Wirkungsbezogener Risikobegriff,
- Mathematisches Wahrscheinlichkeitsmodell.

Ohne Risiko explizit zu definieren, zeigt das **extensive Risikoverständnis** dessen betriebswirtschaftliche Bedeutung auf. Es beschreibt Risiko als einen mit dem unternehmerischen Handeln untrennbar verbundenen Sachverhalt (vgl. Mensch 1991, S.1). Risiko gilt als ständige Begleiterscheinung jedes Wertschöpfungsprozesses (vgl. Neubeck 2003, S.14). Dieser umfasst sowohl primäre Aktivitäten der Wertkette, wie Forschung und Entwicklung, Produktion und Vertrieb, als auch sekundäre Aktivitäten wie die Unterstützung durch Informationstechnologie (vgl. Porter 2000, S.73f.). Im Rahmen dieser Arbeit wird ausschließlich der Begriff Wertkette als direkte Übersetzung von „Value Chain“ verwendet. Alternativ wird in der Literatur auch der Begriff Wertschöpfungskette verwendet, eine Differenzierung der Begriffe erfolgt hier nicht (vgl. Volck 1997, S.18ff.). Der im Rahmen dieser Arbeit verwendeten Risikodefinition liegt das extensive Risikoverständnis zugrunde, da das Zusammenspiel von Risiko und Wertschöpfung besonders aus bankinterner Sicht eine entscheidende Rolle spielt. Dieses Risikoverständnis ist jedoch zu allgemein, um eine Quantifizierbarkeit der Risiken zu gewährleisten.

Daher wird auch der **ursachenbezogene Risikobegriff** erläutert. Dieser verbindet nach Fasse (1995) die zwei Komponenten Entscheidung und Information. Alternativ kann hier auch getrennt vom informations- beziehungsweise entscheidungsbezogenen Risikobegriff gesprochen werden (vgl. Imboden 1983, S.45ff.; Sitt 2003, S.8f.). Die entscheidungsorientierte Sichtweise (vgl. Heinen 1966, S.160ff.) hebt den Aspekt der Entscheidungsfindung für die Ableitung einer Risikodefinition hervor. Risiko ist hiernach die Gefahr, im Entscheidungsprozess aufgrund der Informationslage eine nicht gewinnoptimierende Alternative zu wählen (vgl. Imboden 1983, S.45f.).

Entscheidungen werden in diesem Kontext ferner nach dem Grad der vorhandenen Informationen in drei Kategorien unterteilt (vgl. Tabelle 2.1):

Grad der Information		
vollständig	**teilweise**	**unbekannt**
Entscheidung unter Sicherheit	Entscheidung unter Risiko	Entscheidung unter Unsicherheit

Tabelle 2.1: Entscheidungssituationen
(vgl. Mag 1977, S.21ff.; Fasse 1995, S.47f.)

Bei Entscheidungen unter Sicherheit ist das Eintreten einzelner Szenarien als sicher anzusehen, wohingegen bei Entscheidungen unter Risiko die Eintrittswahrscheinlichkeit ex ante bekannt ist (vgl. Kupsch 1973, S.26ff.). Von Entscheidungen unter Unsicherheit wird gesprochen, wenn keine Eintrittswahrscheinlichkeiten bekannt sind. Im Rahmen dieser Arbeit wird Risiko entsprechend der Interpretation von Knight als messbare Ungewissheit betrachtet (vgl. Knight 1965, S.20). Eine Entscheidung unter Sicherheit stellt eine starke Vereinfachung der Problemstellung dar (vgl. Eisenführ und Weber 2003, S.20), die, genauso wie die Entscheidung unter Unsicherheit, für quantitative Modelle ungeeignet erscheint. Daher wird die Entscheidung unter Risiko als weitere Grundlage für den Risikobegriff gewählt.

Beim **wirkungsbezogenen Risikobegriff** steht die Abweichung von einem Sollzustand im Vordergrund (vgl. Fasse 1995, S.52; Neubeck 2003, S.17). Hierbei wird *„[...] Risiko auch mit der Gefahr einer negativen Abweichung von einem absoluten oder relativen Ziel gleichgesetzt“* (Schuy 1989, S.18). Das bedeutet, dass ausschließlich ein negatives Abweichen, also ein möglicher Verlust, als Risiko bezeichnet wird. Chancen werden hierbei bewusst ignoriert. In diesem Sinne ist Risiko die mögliche Abweichung vom Plan, die mit einem Verlust verbunden ist (vgl. Braun 1984, S.22f.).

Um **mathematische Wahrscheinlichkeitsmodelle** anwenden zu können, ist die Entscheidung unter Risiko eine notwendige Annahme. Die formale Struktur für einen Zufallsvorgang wird durch den Wahrscheinlichkeitsraum (Ω, $\mathcal{F}$, P) definiert (vgl. Sandmann 1999, S.101ff.). Dieser umfasst einen Zustandsraum Ω, also die Menge der Elementarereignisse eines Zufallsexperiments. Damit eng verbunden ist die σ-Algebra $\mathcal{F}$ als ein System aus Teilmengen der Elementarereignisse aus Ω. Die Funktion P ist das Wahrscheinlichkeitsmaß, das jedem Ereignis eine Eintrittswahrscheinlichkeit zuordnet. Diese Ereignisse entspre-

chen dabei zukünftigen Szenarien oder Umweltzuständen. Der mathematische Begriff des Wahrscheinlichkeitsraums ist daher eng mit der Entscheidung unter Risiko verbunden, da über die Wahrscheinlichkeiten die Entscheidungssituation beschrieben werden kann (vgl. Fasse 1995, S.47f.). Um die Quantifizierbarkeit in das Risikoverständnis zu integrieren, wird der Wahrscheinlichkeitsraum als Bestandteil des Risikobegriffs festgelegt. Ferner sind mathematische Wahrscheinlichkeitsmodelle die zentrale Grundlage für ein auf funktionalen Zusammenhängen und Wahrscheinlichkeitsverteilungen basierendes Risikomodell.

Zusammengefasst beinhaltet der im Rahmen dieser Arbeit verwendete allgemeine Risikobegriff negative Auswirkungen aus sämtlichen Teilelementen der unternehmerischen Wertkette und basiert auf Entscheidungen unter Risiko. Formal baut der Risikobegriff auf einem mathematischen Wahrscheinlichkeitsraum auf.

Definition (2.1): Das allgemeine Geschäftsrisiko wird als möglicher negativer finanzieller Effekt im gesamten Umfeld der Wertkette interpretiert, der aufgrund zufallsverteilter Einflussgrößen mit einer ex ante bekannten Wahrscheinlichkeit eintreten kann.

Beispiele für Risiken, die dieser Definition entsprechen, sind entgangene Gewinnmöglichkeiten aufgrund einer falschen Produktentwicklung, eine zu hohe Fehlerquote in der Abwicklung oder Umsatzeinbußen in einem bestimmten Marktsegment. Der allgemeine Risikobegriff ist jedoch für das Management der Technologierisiken nicht ausreichend spezifisch. Aus diesem Grund wird der Begriff über eine Definition der operationellen Risiken weiter konkretisiert.

2.1.2 Operationelle Risiken

In Abgrenzung zu den klassischen Geschäftsrisiken stellen operationelle Risiken Verluste aus dem Betrieb der Kerngeschäftsprozesse dar (vgl. King 2001, S.7; Leippold, Doebli und Vanini 2003, S.4). Der englische Begriff „Operational Risk“ wird hier ausschließlich mit operationelles Risiko übersetzt. Die alternative Bezeichnung operationale Risiken ist synonym zu verstehen. Ein Verlust aus operationellen Risiken entsteht beispielsweise durch einen Verfahrensfehler oder einen technisch bedingten Ausfall und ist unabhängig von dem den Geschäftsprozessen inhärenten Risiko. Zunächst wird die begriffliche Entwicklung im Bereich der Kreditinstitute aufgezeigt und daraus die für diese Arbeit verwendete Definition operationeller Risiken abgeleitet.

„Operational risk is nothing new. It has always been the first risk that banks have to manage – before they make their loan or execute their first trade.“ (Wills 1999, S.52)

Operationelle Risiken werden teilweise als bereits immer existent beschrieben. Als verhältnismäßig neu jedoch kann die Aufnahme der operationellen Risiken in die Disziplin des Risikomanagements betrachtet werden: *„What is new, though, is the idea that operational risk management is a discipline in itself with its own management structure, tools and processes, much like credit or market risk“* (Wills 1999, S.52). Grundlage des Managements operationeller Risiken ist eine eindeutige Definition (vgl. Minz 2004, S.13). Im Laufe der Entwicklung des Verständnisses operationeller Risiken unterlag der Begriff stetiger Veränderungen:

- Begriff des Organisations- bzw. Betriebsrisikos
- Definition der „Group of 30“ (1993 in den USA)
- Residualdefinition (1998 von der EU)
- Internationale Studie zum Begriff (BBA, ISDA und RMA 1999)
- Definition des Basler Ausschusses

Ursprünglich findet sich in der deutschsprachigen Literatur anstelle der Bezeichnung operationelle Risiken häufig der Begriff des **Organisations- bzw. Betriebsrisikos** (vgl. Fürer 1990, S.73f.; Karl 1996, S.8; Rode und Moser 1999, S.721). Dieser beinhaltet beispielsweise Verluste aus menschlichem beziehungsweise systemtechnischem Versagen oder unzulänglichen Verfahren und internen Kontrollen (vgl. Scharpf und Luz 2000, S.119f.). In der Rechtsprechung bezeichnet der Begriff allgemein Betriebsstörungen, die weder vom Arbeitgeber noch vom Arbeitnehmer zu verantworten sind (vgl. Berger 1980; BGB § 615).

Im angelsächsischen Bereich liefert die **„Group of 30“**, eine non-profit Organisation internationaler Kreditinstitute, öffentlicher Banken und Universitäten, 1993 eine Definition für operationelle Risiken. Hiernach ist operationelles Risiko *„the risk of losses occurring as a result of inadequate Systems and control, human error, or management failure“* (GO30 1993). Diese Definition unterteilt operationelle Risiken in die Bereiche Menschen, Systeme, Prozesse und Management. Die Bedeutung des Managements wird somit explizit hervorgehoben. Es liegt dabei die Annahme zugrunde, dass Managemententscheidungen einen wesentlichen Einfluss auf operationelle Risiken haben (vgl. Utz 2002, S.101).

Eine allgemeine **Residualdefinition**, bei der operationelle Risiken alle Risiken subsumieren, die nicht die klassischen Risiken des Bankgeschäfts sind, schlägt die EU 1999 vor (siehe EU 1999). Hier werden sonstige Risiken als *„alle Risiken, die nicht Kreditrisiken, Marktrisiken oder Zinsänderungsrisiken (im Bankbestand) sind“* (EU 1999, Tz.35), definiert. Das umfasst sowohl Betriebs- und

Rechtsrisiken als auch beispielsweise Reputationsrisiken. Diese Residualdefinition scheint jedoch zu allgemein, um ein ursachengerechtes Management der operationellen Risiken zu ermöglichen (vgl. Jörg 2002, S.5; Minz 2004, S.15).

Eine **internationale Studie** der British Bankers' Association (BBA), International Swaps and Derivatives Association (ISDA) und der Robert Morris Association (RMA) hat 1999 die Verbreitung unterschiedlicher Definitionen für operationelle Risiken bei internationalen Kreditinstituten untersucht. Danach wird eine Positivdefinition von einer Mehrzahl der Kreditinstitute bevorzugt. Obwohl die einzelnen Institute unterschiedliche Begriffe verwenden, kann folgender Konsens festgestellt werden: *„Operational risk is the risk of direct or indirect loss resulting from failed or inadequate processes, systems, people or from external events.“* (Wills 1999, S.52).

Eine weitere Definition stellt der Ansatz des **Basler Ausschusses** dar, der operationelles Risiko als *„[...] the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.“* (Basel II, Tz.644) definiert. Entgegen der originären Fassung im Konsultationspapier (vgl. BCBS 2001, S.2) wird die Formulierung der direkten und indirekten Verluste hier nicht mehr verwendet. Prozessrisiken ergeben sich aus einem falschen Aufbau der Geschäftsprozesse, wie zum Beispiel der fehlenden Integration notwendiger Kontrollen in den Arbeitsablauf. Risiken aus menschlichem Versagen sind als bewusste oder versehentliche, fehlerhafte Handlungen der Mitarbeiter zu interpretieren. Operationelle Risiken aus Systemen resultieren aus Schwächen in den Anwendungssystemen selbst sowie aus allgemeinen Fehlern bei der Nutzung von Informationstechnologie. Risiken aus externen Ereignissen entsprechen Verlusten aus Naturkatastrophen oder Terroranschlägen. Das rechtliche Risiko schließt diese Definition indirekt mit ein, strategische und Reputationsrisiken werden hierdurch jedoch nicht berücksichtigt: *„This definition includes legal risk, but excludes strategic and reputational risk“* (Basel II, Tz.644). Ein Ausschluss der Strategierisiken erscheint hier sachgemäß, da diese die langfristige Grundlage für den Geschäftsbetrieb darstellen und nicht aus dem Betrieb selbst resultieren.

Die Definition des Basler Ausschusses unterscheidet sich in mehreren Punkten von den vorhergehenden Ansätzen. Managementfehler werden nur implizit durch den Begriff menschliches Versagen mit eingeschlossen, indirekte Risiken sind nicht enthalten. Ferner basiert die Definition auf einer eindeutigen Nennung der einzelnen Teilkategorien. Hierin sind auch Bedrohungen durch externe Ereignisse enthalten. Im Sinne der historischen Kritik, die verwendeten Definitionen seien noch nicht einheitlich (vgl. Van den Brink 2001, S.1; Piaz 2002. S.58ff.; Minz 2004, S.13), ist abzuwarten, ob das Basler Verständnis auch einen betriebswirtschaftlichen Standard prägen wird. Da die Definition des Basler

Ausschusses jedoch die Grundlage für die aufsichtsrechtliche Unterlegung mit Eigenmitteln darstellt und somit bindenden Charakter haben wird, wird sie als Basis dieser Arbeit verwendet.

Definition (2.2): Operationelles Risiko ist ein aus dem Betrieb der Geschäftsprozesse resultierender möglicher negativer finanzieller Effekt und wird gemäß der Ursächlichkeit in die vier Risikokategorien Prozessfehler, Human-Risiken, Technologierisiken und externe Ereignisse untergliedert.

Operationelle Risiken können auch als ein Zusammenwirken von Ursachen, Ereignissen und Effekten betrachtet werden (vgl. Dowd 2003, S.37ff.). Ein Ereignis ist dann ein konkreter Vorfall (z.B. eine Störung im Bankbetrieb), der sich einer bestimmten Ursache (z.B. ein Systemausfall) zuordnen lässt. Der Effekt wiederum stellt den messbaren Einfluss auf die Ertragssituation (z.B. eine erforderliche Abschreibung) dar.

2.1.3 Grundlegende Risikomaße

Zur Quantifizierung der eingegangenen Risiken existieren unterschiedliche Risikomaße. Die in diesem Kapitel dargestellten Risikomaße beziehen sich auf das in Definition 2.1 festgelegte Risikoverständnis. Der Schwerpunkt liegt aufgrund der Annahme einer ex ante bekannten Wahrscheinlichkeit auf den verteilungsbasierten Risikomaßen. Eine Darstellung der Ansätze aus der Erwartungsnutzentheorie erfolgt nicht, hierzu wird auf die Literatur verwiesen (vgl. Guthoff, Pfingsten und Wolf 1998, S.114ff.; Liekweg 2003, S.68ff.). Zentrale Grundlage für die Quantifizierung des Risikos ist die zugrunde liegende Verteilung der Verluste. Die Wahrscheinlichkeitsverteilung einer stetigen Zufallsvariablen X wird über ihre Dichtefunktion $f_X(x)$ beschrieben.

$$\int_a^b f_X(x)\,dx = P(a \le X \le b) \quad \text{mit} \quad \int_{-\infty}^{\infty} f_X(x)\,dx = 1 \tag{2.1}$$

Dabei ist $f_X(x)$ eine positive, integrierbare Funktion. Häufig kann jedoch die Verlustverteilung nicht direkt analytisch ermittelt werden. Zur Berechnung werden dann Simulationen auf Basis historischer Daten oder parametrisierter Verteilungen verwendet (vgl. Gruber 2001, S.88). Als Simulation wird im Rahmen dieser Arbeit die automatische Generierung von Szenarien verstanden (vgl. Straßberger 2002, S.106). Eine technische Beschreibung des Simulationsbegriffs erfolgt in Kapitel 2.3.3.

Bei einer historischen Simulation werden vergangene Realisationen als Szenarien verwendet und somit reale historische Werte für die Einflussgrößen in die Verlustfunktion eingesetzt, um hieraus zukünftige Verluste zu simulieren. Dieser Vorgehensweise liegt indirekt die Annahme zugrunde, dass der stochastische Prozess für die Einflussgrößen stationär ist (vgl. Straßberger 2002, S.106). Ein Vorteil der historischen Simulation ist, dass keine Annahmen über die zugrunde liegenden Verteilungen notwendig sind und keine Parameter geschätzt werden müssen (vgl. Straßberger 2002, S.108). Als nachteilig ist anzusehen, dass eine umfangreiche historische Datenbasis benötigt wird und strukturelle Veränderungen eventuell ignoriert werden (vgl. Picoult 1999, S.35).

Die parametrische Simulation unterscheidet sich von der historischen Simulation in der Erzeugung der Werte für die Einflussgrößen. Die Ausprägungen werden zufällig über eine vorgegebene Verteilung simuliert. Falls bereits historische Daten vorliegen, können hieraus die Verteilungsparameter der Risikofaktoren geschätzt werden. Der Vorteil der parametrischen Simulation ist ihre universelle Einsatzfähigkeit, da hierdurch sämtliche Aspekte einer Verteilung berücksichtigt werden können (vgl. Straßberger 2002, S.111). Hierin liegt jedoch gleichzeitig auch eine Schwäche, da das Modellrisiko mit zunehmender Anzahl getroffener Annahmen stetig steigt (vgl. Straßberger 2002, S.112).

Bei der Wahl des Risikomaßes ist zu beachten, dass in der Regel eine Kenngröße allein nicht alle Risikoaspekte abdecken kann und so möglicherweise ein Informationsverlust entsteht (vgl. Haaß 2001, S.12). Im Folgenden werden die Risikomaße Varianz, Lower Partial Moments, Value at Risk (VaR) sowie der Conditional Value at Risk (CVaR) vorgestellt.

a Varianz

Ein Maß für die Streuung einer Zufallsvariablen um den Mittelwert liefert die Varianz (vgl. Bomsdorf 1995, S.43). Dieser Wert kann als Volatilität einer Messgröße bezeichnet werden. In diesem Sinne stellt das Risiko die Streubreite der möglichen Werte dar. Eine geringe Streuung impliziert Sicherheit, eine hohe Streuung stellt ein ausgeprägtes Risiko dar. Die Varianz V einer stetigen Zufallsvariablen X ist aufbauend auf dem Erwartungswert E wie folgt definiert:

$$V(X) = \int_{-\infty}^{\infty} (x - E(X))^2 f_X(x)\,dx \qquad \text{mit} \qquad (2.2)$$

$$E(X) = \int_{-\infty}^{\infty} x\, f_X(x)\,dx$$

Für die Ermittlung des Risikos über Varianzen ist die Kenntnis der zugrunde liegenden Verteilung der Zufallsvariablen oder zumindest eine große Anzahl an Messwerten erforderlich (vgl. Bessis 2002, S.83). Die Anwendung der Varianz als Risikomaß findet sich beispielsweise in der Portfoliotheorie von Markowitz. Die Messung des Risikos über die Varianz ist jedoch nicht mit dem Risikobegriff entsprechend Definition 2.1 konform, da mögliche positive Abweichungen gleichermaßen als Risiko im Sinne von Unsicherheit interpretiert werden. Für symmetrische Verteilungen bedeutet eine hohe Varianz dann gleichzeitig ein hohes Verlust- und Gewinnpotential. Bei asymmetrischen Verteilungen kann aus einer Veränderung der Varianz grundsätzlich keine nach Verlusten und Gewinnen differenzierende Betrachtung durchgeführt werden (vgl. Albrecht und Maurer 2002, S.108).

b Lower Partial Moments

Aus diesem Grund werden hier Risikomaße dargestellt, die ausschließlich die möglichen Verluste miteinbeziehen. Risikomaße, die ausschließlich negative Abweichungen berücksichtigen und mögliche Gewinne ignorieren werden als „Downside risks“ oder Shortfall-Maße bezeichnet (vgl. Bessis 2002, S.84). Die formale Grundlage bilden die Lower Partial Moments, die grundsätzlich über folgende Formel definiert werden:

$$LPM_k = \int_{-\infty}^{\tau} (\tau - x)^k f_X(x)\,dx, \qquad k \geq 0 \tag{2.3}$$

Für den Fall $k = 0$ ergibt sich die sogenannte Shortfall-Wahrscheinlichkeit. Dies ist die Wahrscheinlichkeit, mit der eine finanzielle Größe eine bestimmte Vorgabe τ unterschreitet (vgl. Straßberger 2002, S.52). Die Shortfall-Wahrscheinlichkeit entspricht der Wahrscheinlichkeitsmasse unterhalb der Vorgabe (vgl. Albrecht und Maurer 2002, S.109). Bei diesem Risikomaß bleibt jedoch die Höhe der jeweiligen Unterschreitung unberücksichtigt. Es wird ausschließlich die Wahrscheinlichkeit für eine Unterschreitung untersucht. Über das Ausmaß der Unterschreitung gibt ein weiteres Lower Partial Moment Auskunft (vgl. Straßberger 2002, S.52). Für $k = 1$ ergibt sich der erwartete Verlust, auch als Shortfall-Erwartungswert bezeichnet. Dieser ist eine Kennzahl für den Betrag, mit dem eine Zielgröße im Mittel unterschritten wird. Bei der Vorgabe des Zielwerts $\tau = 0$ ergibt sich direkt der mittlere, absolute Verlust. Das Lower Partial Moment mit $k = 2$ beschreibt die Ausfallvarianz, also die Streuung der Ausfälle unterhalb des Schwellenwertes. Mathematisch sind Lower Partial Moments mit Werten von $k = 0$ bis unendlich möglich, betriebswirtschaftlich sind jedoch nur die Werte $k = 0$, 1 oder 2 sinnvoll (vgl. Oehler und Unser 2001, S.22).

Bei den Shortfall-Risikomaßen wird von einer festgelegten Verlustgrenze ausgegangen. Der Zielwert wird vorgegeben und die Wahrscheinlichkeit für eine Unterschreitung, die mittlere Unterschreitung oder die Ausfallvarianz ermittelt.

c Value at Risk

Eine andere Betrachtungsweise stellt die Untersuchung der Quantile einer Verlustverteilung dar. Im Bereich der Marktrisiken findet besonders der VaR als Risikomaß Verwendung (siehe Allen, Boudoukh und Saunders 2004). Obgleich das Konzept bereits älter ist, wird die aktuelle Popularität im Wesentlichen der Entwicklung von RiskMetrics durch JP Morgan zugeschrieben. Der VaR sollte ursprünglich eine Antwort auf die einfache Frage nach den möglichen Verlusten innerhalb des nächsten Handelstages geben: *„[...] how much can we loose in our trading portfolio by tomorrow close?“* (Allen, Boudoukh und Saunders 2004, S.4). Allgemein wird der VaR als der maximale Verlust bezeichnet, der mit einer vorgegebenen Wahrscheinlichkeit nicht übertroffen wird (vgl. Bessis 2002, S.87). Es wird hierzu ein Konfidenzniveau *p* (z.B 99,9%) vorgegeben und darauf basierend die Verlustobergrenze ermittelt. Mit einer Wahrscheinlichkeit in Höhe des Konfidenzniveaus wird dieser Verlust innerhalb eines bestimmten Zeitintervalls nicht überschritten. Der VaR ist ausdrücklich nicht als maximal möglicher Verlust sondern nur als Schätzer des maximalen Verlustes unter normalen Marktkonditionen zu betrachten (vgl. Studer 1998, S.55).

Formal definiert ist der *VaR* die Verlustobergrenze einer durch die Dichtefunktion $f_X(x)$ vorgegebenen Verlustverteilung, die mit der Wahrscheinlichkeit *p* nicht überschritten wird (vgl. Straßberger 2002, S.61):

$$VaR = F_X^{-1}(p) \quad \text{mit} \quad F_X(VaR) = \int_{-\infty}^{VaR} f_X(x)\,dx = p \tag{2.4}$$

Die Verlustverteilung modelliert dabei die Wertentwicklung des zu betrachtenden Objekts (z.B. ein Portfolio) auf Basis messbarer, stochastischer Einflussgrößen (z.B. Kursschwankungen).

Zur Berechnung des VaR existiert neben den Simulationsmethoden auch noch das Delta-Normal-Modell (auch Varianz-Kovarianz-Modell) (vgl. Gruber 2001, S.88). Dieses setzt voraus, dass die Einflussgrößen normalverteilt sind und die Verlustfunktion näherungsweise linear über die Einflussgrößen beschrieben werden kann (vgl. Studer 1998, S.56). Mögliche negative Wertveränderungen werden als Varianz der Verlustverteilung aus den Einzelvarianzen der Risikofaktoren über das 1. Glied einer Taylor-Reihe linear approximiert. Diese Metho-

de kann über die Verwendung weiterer Terme der Taylor-Reihe verfeinert werden. Für operationelle Risiken scheint das Delta-Normal-Modell nicht anwendbar, da von einer Standardnormal-Verteilung der operationellen Verluste oder der verursachenden Einflussgrößen nicht ausgegangen werden kann (vgl. Danielsson et al. 2001, S.9).

Ein wesentlicher Nachteil des VaR für operationelle Risiken ist, dass keine Erkenntnisse über die Verteilung der Verluste oberhalb des VaR gewonnen werden (vgl. Chong 2004, S.27). Gerade für operationelle Risiken kommt diesen seltenen, jedoch den Fortbestand des Unternehmens gefährdenden Verlusten, eine hohe Bedeutung zu (vgl. Danielsson et al. 2001, S.9). Eine weitere Einschränkung des VaR bezieht sich auf die nicht erfüllte Subadditivität. Der VaR eines Portfolios ist nicht zwangsläufig geringer als die Summe der VaR der einzelnen Teilportfolios. Trotz der bekannten Schwächen ist der VaR – auch im Umfeld operationeller Risiken – ein im bankweiten Risikomanagement verbreitetes Risikomaß und wird daher auch im Rahmen dieser Arbeit verwendet.

d Conditional Value at Risk

Grundsätzlich steht ein konkretes Risikomaß stets im Bezug zu einer bestimmten Fragestellung. Eine globale Klassifizierung von Risikomaßen im Hinblick auf ihre Qualität scheint daher nicht möglich (vgl. Haaß 2001, S.13). In der Literatur werden unter dem Begriff kohärente Risikomaße jedoch allgemeine Anforderungen an ein Risikomaß zusammengefasst (vgl. Artzner et al. 1997, S.68). Der Begriff kohärent wird dabei vom englischen „coherent“ abgeleitet und bedeutet übertragen sinngebend oder sinnvoll. Ein Risikomaß wird genau dann als kohärent bezeichnet, wenn es die Eigenschaften der Translationsinvarianz, der Subadditivität, der positiven Homogenität und der Monotonie erfüllt (vgl. Artzner et al. 1999, S.209f.). Die Translationsinvarianz (vgl. Formel 2.5) impliziert, dass bei einer Ergänzung des bestehenden Portfolios A um eine Anlage a zum risikolosen Zins r das Gesamtrisiko ρ in der gleichen Höhe reduziert wird. Im Hinblick auf eine regulatorische Eigenmittelunterlegung sollte ein Risikomaß demnach eine risikolose Anlage honorieren und eine entsprechend geringere Risikovorsorge verlangen (vgl. Barth 2000, S.90).

$$\rho(A+a\,r)=\rho(A)-a \tag{2.5}$$

Die Bedingung der Subadditivität (vgl. Formel 2.6) besagt, dass durch die Kombination zweier risikobehafteter Positionen A und B kein zusätzliches Risiko entstehen kann. Im Umkehrschluss bedeutet es, dass durch Trennen einer Position die Risiken nicht reduziert werden dürfen. In diesem Zusammenhang wird auch vom Diversifikationseffekt gesprochen. Das Gesamtrisiko ist maximal die

Summe seiner Einzelrisiken, falls diese nicht korreliert sind. Andernfalls ist das Gesamtrisiko aufgrund von Diversifikationseffekten sogar geringer (vgl. Acerbi und Tasche 2001, S.3).

$$\rho(A+B) \leq \rho(A)+\rho(B) \tag{2.6}$$

Die Positive Homogenität (vgl. Formel 2.7) impliziert, dass die Veränderung des Wertes einer Position *A* um einen Faktor λ, stets eine Änderung des Risikos um denselben Faktor zur Folge hat. Dies ist als ein Spezialfall der Subadditivität zu betrachten.

$$\rho(\lambda A) = \lambda \rho(A) \tag{2.7}$$

Im Sinne von kohärenten Risikomaßen bedeutet Monotonie (vgl. Formel 2.8), dass für ein Portfolio *A*, dessen Wertentwicklung grundsätzlich unterhalb der eines anderen Portfolios *B* liegt, das Risiko von Portfolio *A* größer sein muss.

$$\rho(B) < \rho(A) \quad \forall A < B \tag{2.8}$$

Im Allgemeinen sind sämtliche quantilbasierten Risikomaße nicht kohärent (vgl. Barth 2000, S.91). Eine Alternative stellen erwartungswertbasierte Risikomaße dar. Zum Beispiel ist das erste Lower Partial Moment, also der Shortfall-Erwartungswert, ein kohärentes Risikomaß (vgl. Straßberger 2002, S.65).

Eine Kombination des Shortfall-Erwartungswertes mit dem VaR ist der Conditional VaR (CVaR), auch Tail-VaR genannt. Hierbei wird der VaR als Verlustobergrenze für das erste Lower Partial Moment verwendet (vgl. Straßberger 2002, S.135f.). Der CVaR ist somit die erwartete Überschreitung des VaR, also zum Beispiel für einen auf 99% bezogenen VaR der Durchschnitt der 1% größten Verluste. Folgende Formel 2.9 definiert den CVaR formal:

$$CVaR = \int_{VaR}^{\infty} (x - VaR) f_X(x) dx \tag{2.9}$$

Da das Konzept des VaR das Kriterium der Subadditivität nicht in jedem Fall erfüllt, ist der VaR kein kohärentes Risikomaß (vgl. Read 1998, S.28). Im Fall der Technologierisiken könnte dies bedeuten, dass durch die getrennte Betrachtung einzelner Bereiche der IT-Landschaft das Gesamtrisiko reduziert wird. Aus Sicht der Bankenregulierung wird damit dem Aspekt der Risikostreuung oder Diversifikation nicht ausreichend Rechnung getragen (vgl. Acerbi und Tasche 2001, S.3). Der VaR wird im Rahmen dieser Arbeit nicht als alleiniges Risikomaß verwendet, sondern stets durch den CVaR ergänzt.

2.2 Risikomanagement in Kreditinstituten

Kreditinstitute haben im Vergleich zu Industrieunternehmen eine hervorgehobene Bedeutung für die gesamte Volkswirtschaft. Das kann im Wesentlichen mit deren Einfluss auf die Geldversorgung und Preisstabilität begründet werden (vgl. Hartmann-Wendels, Pfingsten und Weber 2004, S.363; Süchting und Paul 1998, S.455ff.). Die originären Aufgabenbereiche eines Kreditinstitutes umfassen das Einlagengeschäft, die Kreditvergabe, den Zahlungsverkehr sowie den Handel in eigenen Positionen. Jede dieser Tätigkeiten ist mit allgemeinen und operationellen Risiken verbunden, die hohe finanzielle Verluste induzieren können. Hiervon sind dann neben den Anforderungen des Staates auch die Ansprüche der Einleger und der Eigenkapitalgeber betroffen. So besteht für alle Stakeholder ein hohes Interesse an einem funktionierenden Risikomanagement, um dadurch den Fortbestand des Kreditinstitutes zu sichern.

Nachfolgend wird das Geschäftsmodell der Kreditinstitute unter gesetzlichen und betriebswirtschaftlichen Gesichtspunkten dargestellt. Darauf aufbauend werden die in Kapitel 2.1.2 definierten operationellen Risiken in die Risikolandschaft des Kreditinstitutes eingeordnet. Abschließend werden der inhaltliche und organisatorische Aufbau des Risikomanagements sowie die regulatorischen Rahmenbedingungen im Hinblick auf operationelle Risiken diskutiert.

2.2.1 Begriffliche Einordnung

Voraussetzung für eine Betrachtung des Risikomanagements operationeller Risiken bei Kreditinstituten ist eine gesetzliche Definition und ein betriebswirtschaftliches Verständnis von Kreditinstituten. Im allgemeinen Sprachgebrauch sowie in dieser Arbeit wird häufig der nicht formale Begriff Bank synonym verwendet. Einleitend wird die Legaldefinition gemäß deutscher Rechtsprechung aufgeführt, um darauf aufbauend das Geschäftsmodell von Kreditinstituten zu analysieren.

Definition (2.3): *„Kreditinstitute sind Unternehmen, die Bankgeschäfte gewerbsmäßig oder in einem Umfang betreiben, der einen in kaufmännischer Weise eingerichteten Geschäftsbetrieb erfordert.“* (KWG §1 Abs.1)

Als Bankgeschäfte im Sinne des Kreditwesengesetzes (KWG) werden zum Beispiel das Kreditgeschäft, das Einlagengeschäft, das Geldkartengeschäft, das elektronische Zahlungsgeschäft, das Depotgeschäft, das Investmentgeschäft oder das Emissionsgeschäft verstanden (vgl. KWG §1 Abs.1 (1) – (12)).

Abzugrenzen vom Begriff des Kreditinstituts sind Finanzdienstleistungsinstitute und Finanzunternehmen. Als Finanzdienstleistungsinstitute werden solche Unternehmen bezeichnet, die bestimmte Formen des Bankgeschäftes betreiben wie beispielsweise die Anlagevermittlung oder Portfolioverwaltung (vgl. KWG §1 Abs.1a (1) – (7)). Diese Legaldefinition entspricht dem Verständnis einer Investmentbank (vgl. Hartmann-Wendels, Pfingsten und Weber 2004, S.25). Als Finanzunternehmen werden Unternehmen definiert, die keine Institute (Kredit- und Finanzdienstleistungsinstitute) sind und im Wesentlichen Beteiligungen oder Forderungen erwerben, Anlageberatung betreiben oder Leasinggeschäfte anbieten (vgl. KWG §1 Abs.3). Die zentralen Vorschriften des KWG gelten für Institute. Finanzunternehmen sind dagegen weniger stark reguliert. Ist eine genaue Zuordnung nicht möglich, finden die jeweils strengeren Regulierungsvorschriften Anwendung (vgl. Hartmann-Wendels, Pfingsten und Weber 2004, S.24). Im Rahmen dieser Arbeit werden ausschließlich Kreditinstitute betrachtet.

Zusätzlich zur Legaldefinition des Kreditinstituts wird nachfolgend eine betriebswirtschaftliche Betrachtung des Geschäftsmodells von Kreditinstituten vorgenommen. Da sich ein detailliertes Geschäftsmodell aus der Literatur nicht ableiten lässt, wird ein abstraktes Schema vorgestellt (vgl. Abbildung 2.1). Grundlage stellt hierbei das Konzept der Wertkette bestehend aus primären und unterstützenden, sekundären Aktivitäten dar (vgl. Porter 2000, S.66ff.). Als primäre Aktivitäten können die Transaktionsfunktion und die Transformationsfunktion verstanden werden (vgl. Börner 2004, S.169ff.). Die Transaktion umfasst hierbei den gesamten Prozess der externen bankbetrieblichen Leistungserstellung vom Vertrieb bis zur Abwicklung. Als Vertrieb wird beispielsweise die Anlageberatung sowie die Kreditvermittlung gesehen (vgl. Vögtle 1997, S.92). Die Abwicklung umfasst die entsprechende Gewährung des Kredits. Die Transformation bezeichnet die zentrale Steuerung der Geldflüsse im Kreditinstitut, wie den Eigenhandel oder das Risikocontrolling.

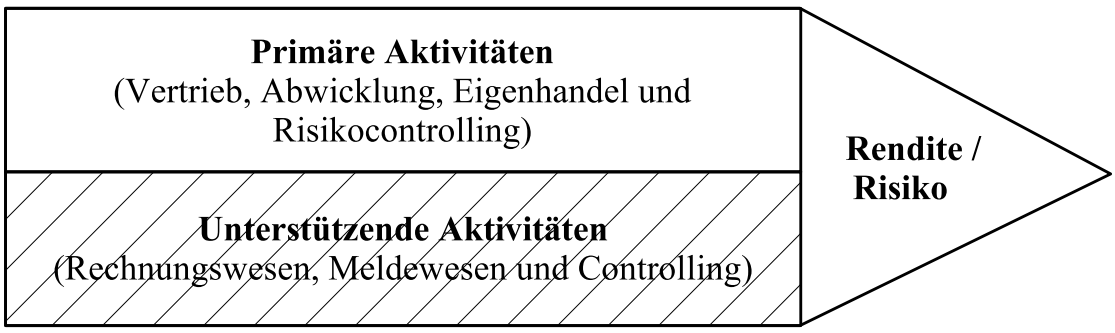

Abbildung 2.1: Abstrakte Wertkette

Die Transaktion und die Transformation entsprechen hier dem Konzept der Kerngeschäftsprozesse (vgl. Lamberti 2004, S.372). Als sekundäre Aktivitäten werden Unternehmensführung und die Bereitstellung einer Infrastruktur genannt (vgl. Börner 2004, S.179). Hierunter fallen auch das finanzwirtschaftliche Controlling sowie das Rechnungs- und Meldewesen.

Die gewählte Aufteilung der Wertkette kann kontrovers diskutiert werden. Auf Ebene der einzelnen Geschäftsfelder des Kreditinstitutes ist das Verständnis zwangsläufig genauer zu spezifizieren. Im Detail unterscheiden sich beispielsweise die Geschäftsprozesse der Wertpapierabwicklung und der Kreditvergabe erheblich. Auf einer abstrakten Ebene ist das Modell jedoch mit den unterschiedlichen Referenzprozessen zu vereinbaren (vgl. Lubich und Aumer 2003, S.56). Für eine detaillierte Darstellung möglicher Wertschöpfungsarchitekturen wird auf die Literatur verwiesen (vgl. Moormann und Möbus 2004, S.252ff.).

Das allgemeine Geschäftsmodell von Kreditinstituten kann auch anhand von Geschäftsfeldern weiter konkretisiert werden. Für die Einteilung der Geschäftsfelder wird die Aufteilung gemäß Basel II bevorzugt (vgl. Basel II, Anhang 8).

- Das Geschäftsfeld Unternehmensfinanzierung/-beratung (Corporate Finance) umfasst Dienstleistungen im Bereich von Unternehmensübernahmen, Börsengängen und durchgeführten Analysen.
- Der Bereich Handel (Trading & Sales) beinhaltet den klassischen Eigenhandel in festverzinslichen Wertpapieren und Aktien, das Market-Making, das Maklergeschäft für Großkunden sowie das Treasury.
- Das Retail-Geschäft (Retail Banking) ist im Sinne von Basel II als das Privatkundengeschäft in Krediten, Kontoführung, Anlageberatung und Kreditkarten zu verstehen.
- Das Firmenkundengeschäft (Commercial Banking) umfasst die Kreditvergabe und Absatzfinanzierung (Akkreditiv etc.) im Bereich der Firmenkunden.
- Das Geschäftsfeld Zahlungsverkehr- und Wertpapierabwicklung (Payment & Settlement) umfasst den Zahlungsverkehr und die Wertpapierabwicklung für Dritte.
- Das Depot- und Treuhandgeschäft (Agency Services) bezeichnet unter anderem die Wertpapierleihe.
- Die Vermögensverwaltung (Asset Management) beinhaltet die gebundene und offene Verwaltung von Vermögen, kurz auch als Private Equity bezeichnet.
- Das Geschäftsfeld Wertpapierprovisionsgeschäft (Retail Brokerage) umfasst die Ausführung von Kunden-Orders.

2.2.2 Bankspezifische Risiken

Um die Risiken in Kreditinstituten systematisch erkennen und steuern zu können, ist es notwendig, eine trennscharfe Risikokategorisierung vorzunehmen. Hierzu werden die allgemeinen Geschäftsrisiken gemäß Definition 2.1 zunächst auf die bankspezifischen Risiken eingegrenzt, um dann die operationellen Risiken entsprechend Definition 2.2 in diese Risikoklassifizierung einzuordnen. Eine eindeutige Differenzierung und Bezeichnung der unterschiedlichen Bankrisiken lässt sich aus der Literatur nicht ableiten. Jedoch werden zumindest das Liquiditätsrisiko, das Kreditrisiko oder das Marktrisiko als typische Bankrisiken gesehen (vgl. Scharpf und Luz 2000 S.81ff.; Schierenbeck 2003, S.5; Hartmann-Wendels, Pfingsten und Weber 2004, S.541f.). Die folgende Abbildung 2.2 spiegelt eine mögliche Klassifizierung wider.

Auf oberster Ebene werden die Risiken in finanzielle (klassische), operationelle sowie strategische und Reputationsrisiken unterteilt. Die Finanzrisiken ergeben sich dabei direkt aus den Finanzströmen der Transformationsfunktion (vgl. Schierenbeck 2003, S.4). Operationelle Risiken generieren ebenso finanzielle Effekte, resultieren jedoch aus dem Betrieb des Bankgeschäfts.

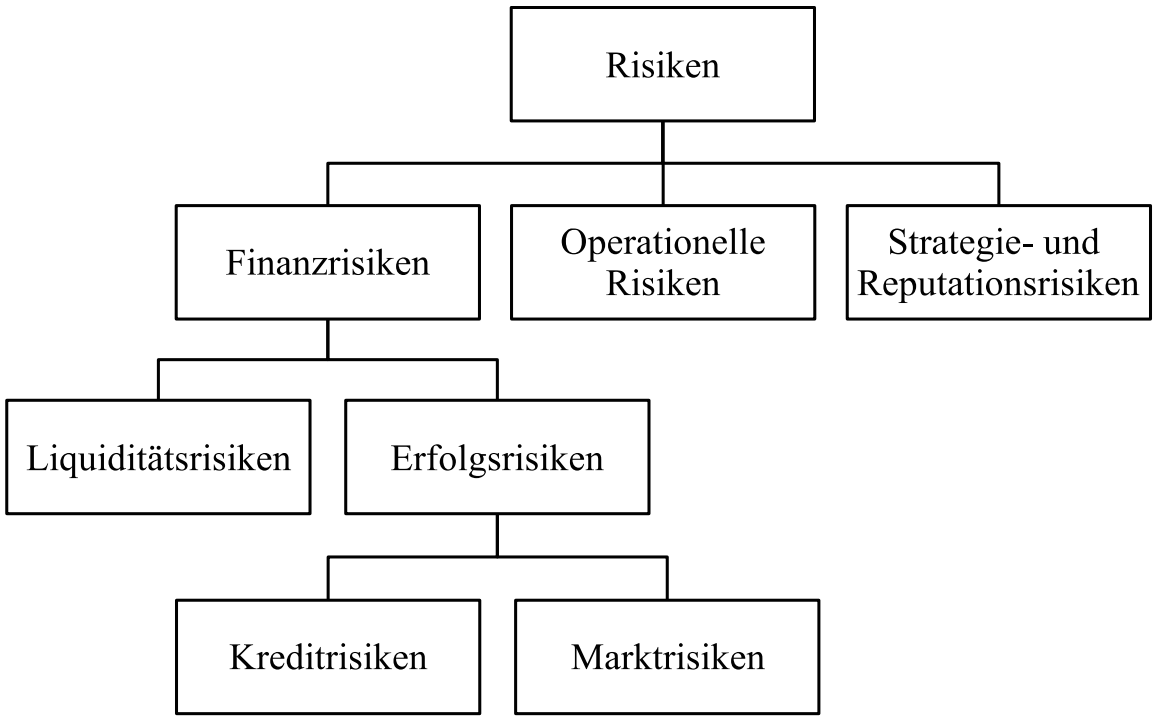

Abbildung 2.2: Risikoklassifizierung
(vgl. Schierenbeck 2003, S.5)

Diese bereits auf der ersten Ebene separierte Betrachtung der operationellen Risiken erscheint insbesondere vor dem Hintergrund zutreffend, dass operationelle Risiken grundsätzlich zusätzlich zu den Finanzrisiken existieren.

Als weitere Risiken werden die Strategie- und Reputationsrisiken gesehen. Diese werden entsprechend der Vorgehensweise des Baseler Ausschusses nicht zu den operationellen Risiken hinzugerechnet. Eine Begründung hierfür ist die unterschiedliche zeitliche Dimension. Während sich operationelle Risiken in der Regel sofort auswirken, beeinträchtigen strategische Risiken den Unternehmenserfolg in der Zukunft. Unabhängig davon sollten jedoch Strategie- und Reputationsrisiken stets Bestandteil eines bankweiten Risikomanagements sein.

Die Finanzrisiken lassen sich in Erfolgs- und Liquiditätsrisiken untergliedern. Liquiditätsrisiken entstehen aus unmittelbaren Forderungen und Fristigkeiten (vgl. Schierenbeck 2003, S.5). Hierfür müssen kurzfristig ausreichend liquide Mittel zur Verfügung stehen, um sämtlichen legitimen Zahlungsverpflichtungen fristgerecht nachkommen zu können (vgl. Bestmann et al. 1997, S.413). Erfolgsrisiken wirken sich langfristig auf die Ertragslage eines Kreditinstituts aus. Eigene finanzielle Mittel wie das Eigenkapital müssen stets ausreichen, um mögliche Verluste tragen zu können.

Die finanziellen Erfolgsrisiken werden als Summe der Kredit- und Marktrisiken gesehen. Die Kreditrisiken bilden sich im Wesentlichen aus dem Kreditportfolio einer Bank, in welchem die Zahlungsunfähigkeit eines Kreditnehmers die Abschreibung des noch ausstehenden Betrags bewirken kann (vgl. Bessis 2002, S.13). Zusätzlich können solche Risiken auch bei Finanzderivaten auftreten, wenn der Kontrahent seinen Verpflichtungen nicht nachkommt. Die Marktrisiken dagegen beschreiben die Gefahr einer negativen Marktentwicklung (vgl. Schierenbeck 2003, S.5). Einflussfaktoren hierfür können Aktienkurse, Zinssätze, Devisenkurse oder Rohstoffpreise sein.

Zusammengefasst stellen die operationellen Risiken, die Liquidäts- sowie die Markt- und Kreditrisiken die zentralen bankspezifischen Geschäftsrisiken dar. Problematisch an dieser Unterteilung ist die Korrelation der unterschiedlichen Risiken, die häufig gemeinsam wirken (vgl. Biermann 2002, S.108). Ein Ansatz ist es, die zu betrachtende Risikoposition derart zu zerlegen, dass die enthaltenen Einzelrisiken sichtbar werden.

Um einen im Sinne der Stakeholder langfristig erfolgreichen und geregelten Geschäftsbetrieb zu ermöglichen, muss das Kreditinstitut sämtliche oben genannten Risiken im Rahmen eines Risikomanagements kontinuierlich analysieren, bemessen und steuern.

2.2.3 Risikomanagement als Prozess

„Im Allgemeinen werden unter dem Begriff Risikomanagement die Ziele und Aufgaben der risikoorientierten Unternehmensführung subsumiert“ (Wolf 2003, S.45). Risikomanagement muss die Umsetzung der Unternehmensziele gewährleisten, indem die den Zielen inhärenten Risiken aktiv kontrolliert werden. Risikomanagement ist demnach als ein direkt die Unternehmensführung unterstützendes Aufgabenfeld anzusehen (vgl. Liekweg 2003, S.10). Aufgrund der möglichen Auswirkungen der Risiken auf den Fortbestand des Kreditinstitutes, ist ein Risikomanagement auch gesetzlich vorgeschrieben. Es sollte jedoch trotz der regulatorischen Notwendigkeit stets auch der betriebswirtschaftliche Nutzen im Vordergrund stehen (siehe Gammelin und Buchhart 2004).

Als Risikomanagement wird die Gesamtheit aller organisatorischer Regelungen und Maßnahmen zur Risikoerkennung und zum Umgang mit den Risiken unternehmerischer Betätigung bezeichnet (vgl. IDW PS 340, Tz.4). Synonym zu dem Begriff Risikomanagement wird häufig auch die Bezeichnung Risikomanagementsystem verwendet (vgl. Neubeck 2003, S.31). Eine definitorische Unterscheidung zwischen den Begriffen (vgl. Grauman 2003, S.553) ist für diese Arbeit nicht von Bedeutung, hierzu wird auf die Literatur verwiesen (vgl. Neubeck 2003, S.23ff.; Martin und Bär 2002, S.82ff.).

Eine eindeutige gesetzliche Regelung, welche Komponenten ein Risikomanagement enthalten sollte, existiert nicht (vgl. Poddig und Kunze 2003, S.694). Es enthält jedoch in der Regel mindestens die Komponenten Frühwarnsystem, Risikocontrolling und Internes Überwachungssystem. Dieses Verständnis (vgl. Abbildung 2.3) ist auch mit den Anforderungen des Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) konform.

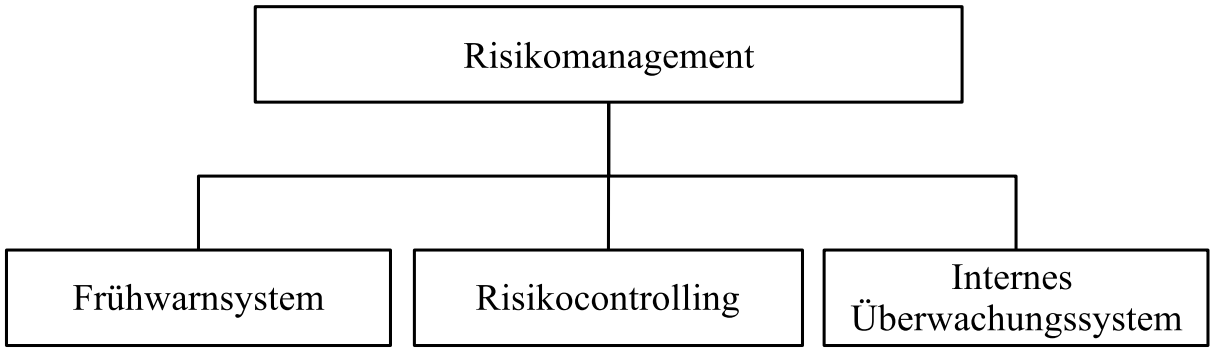

Abbildung 2.3: Risikomanagementsystem
(vgl. Lück 1998, S.9)

Als Frühwarnsysteme werden Instrumente verstanden, die eine rechtzeitige Erkennung von Risiken ermöglichen, so dass eine geeignete Reaktion möglich ist (vgl. Lück 1998, S.11). Hierbei kann zwischen dem operativen und dem strategischen Frühwarnsystem unterschieden werden (vgl. Wolf und Runzheimer 2003, S.53ff.). Das Risikocontrolling ist zentral für die Koordination der Planung, Informationsversorgung, Kontrolle und Steuerung im Bereich des Risikomanagements verantwortlich (vgl. Lück 1998, S.11). Das Interne Überwachungssystem hat die Aufgabe, die Zuverlässigkeit der Geschäftsprozesse unter dem Aspekt der Wirtschaftlichkeit sicherzustellen (vgl. Lück 1998, S.9). Dies umfasst organisatorische Sicherungsmaßnahmen, Prozesskontrollen sowie den Aufbau einer Internen Revision (vgl. Martin und Bär 2002, S.130).

Um die Umsetzung des Risikomanagements organisatorisch zu strukturieren, existieren in der Literatur eine große Anzahl von Vorschlägen. Als Gemeinsamkeit lässt sich jedoch erkennen, dass häufig ein prozessualer Aufbau des Risikomanagements über mehrere Phasen in Form eines Regelkreises verwendet wird (vgl. Liekweg 2003, S.6f.). In diesem Kontext stellt die für diese Arbeit wichtige Quantifizierung einen grundlegenden Bestandteil des Regelkreises dar. Die in der Literatur dargestellten Ansätze legen Anzahl und Inhalt der einzelnen Phasen in der Regel nicht eindeutig fest. Die Ansätze reichen von einer Unterteilung in drei Phasen (vgl. Farny 1979, S.31ff.; Krümmel 1989, S.41ff.), über eine Unterteilung in vier Phasen (vgl. Martin und Bär 2002, S.89; Culp 2002, S.199ff.) bis zu einer Unterteilung in fünf Phasen (vgl. Spellmann 2002, S.28ff.; Neubeck 2003, S.86ff.). Folgende Abbildung 2.4 stellt mögliche Phasen des Risikomanagementprozesses graphisch dar:

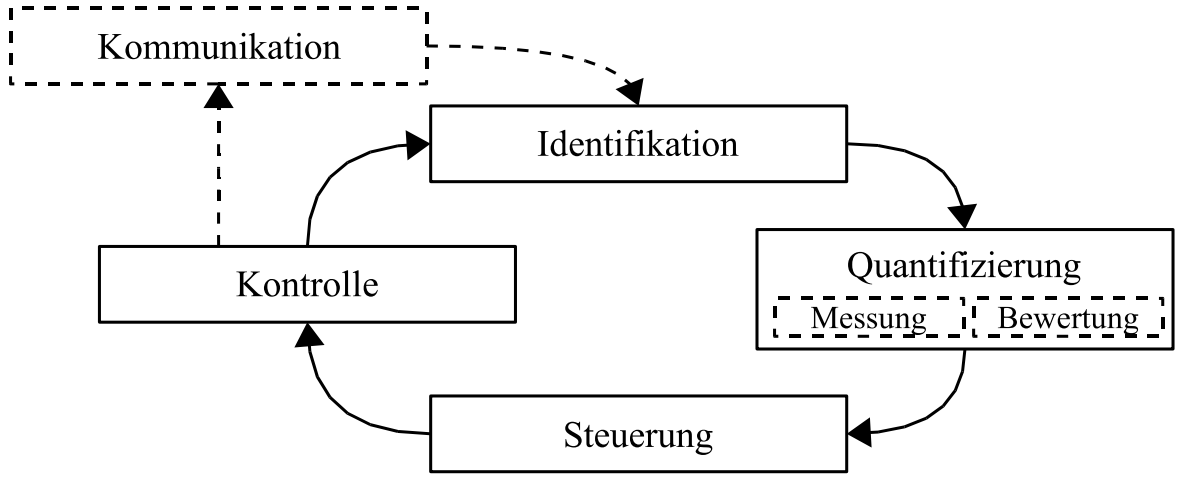

Abbildung 2.4: Risikomanagementprozess

Die Unterschiede in der Anzahl der Phasen resultieren im Wesentlichen daraus, dass die Phase der Quantifizierung in einigen Ansätzen noch weiter in zwei getrennte Teilprozesse Messen und Bewerten untergliedert wird. Teilweise wird zudem eine weitere, separate Phase der Kommunikation eingeführt.

Entscheidende Grundlage für das Risikomanagement ist die **Identifikation** bestehender oder möglicher Risiken. Dazu werden in diesem Teilprozess sämtliche Risikofelder im Umfeld des Kreditinstituts möglichst vollständig ermittelt und analysiert. Die Ergebnisse werden über eine Risikoinventur zusammengefasst (vgl. Neubeck 2003, S.76). Gegebenenfalls sind die Risiken hierbei zu klassifizieren. Von besonderer Bedeutung ist es, nicht nur die Identifikation ausschließlich akuter Risiken zu betreiben, sondern über Frühwarnindikatoren auch mögliche zukünftige Risiken zu berücksichtigen.

Die **Quantifizierung** der Risiken stellt die wesentliche Grundlage für eine aktive Steuerung dar. Durch die Risikoquantifizierung werden das mögliche Ausmaß der finanziellen Effekte identifizierter Risiken bestimmt und die jeweiligen Ursachen analysiert. Dies ermöglicht es dem Unternehmen, adäquat auf die Risiken zu reagieren und beispielsweise dem Verlustpotential ausreichend Eigenkapitalreserven gegenüber zu stellen. Zur sachgerechten Beurteilung der Risiken ist ein geeignetes Risikomaß für die Quantifizierung festzulegen.

Die Phase der **Steuerung** umfasst sämtliche Maßnahmen zum Vermeiden, Vermindern, Abwälzen und Übernehmen von Risiken. Hierbei ist es wichtig, dass die durch getroffene Maßnahmen erreichte Veränderung des Risikopotentials möglichst quantifiziert werden kann. Alternativ ist aber auch eine qualitative Bewertung der Maßnahmen denkbar.

Die **Kontrolle** dient abschließend dazu, den Erfolg der getroffenen Maßnahmen zu überwachen und die Wirksamkeit des Risikomanagements nachhaltig sicherzustellen. Der Risikomanagementprozess ist hierzu als Regelkreis konzipiert, so dass auf erkannte Abweichungen wiederum in der Phase der Identifikation reagiert werden kann.

Die Phase der **Kommunikation** ist in Abbildung 2.4 nur prozessbegleitend enthalten. Da in der Regel eine ständige Berichterstattung an relevante Interessengruppen unterstellt wird, kann der Aspekt der Kommunikation auch allen oben genannten Phasen zugerechnet werden.

Die im Rahmen dieser Arbeit beschriebene Ontologie-zentrierte Vorgehensweise zur Quantifizierung operationeller Technologierisiken ist im Kern der Phase der Quantifizierung zuzurechnen.

2.2.4 Regulierung operationeller Risiken: Basel II

Aufgrund der bereits mehrfach aufgeführten Bedeutung von Kreditinstituten für die gesamte Volkswirtschaft, ist der Betrieb von Bankgeschäften im internationalen Umfeld sowie insbesondere auch in Deutschland staatlich reguliert:

„Die Bundesanstalt hat Missständen im Kredit- und Finanzdienstleistungswesen entgegenzuwirken, welche die Sicherheit der den Instituten anvertrauten Vermögenswerte gefährden, die ordnungsmäßige Durchführung der Bankgeschäfte oder Finanzdienstleistungen beeinträchtigen oder erhebliche Nachteile für die Gesamtwirtschaft herbeiführen können.“ (KWG §6 Abs. 2)

Eine Darstellung theoretischer Ausprägungen der Regulierung sowie eine kritische Diskussion der Widersprüche in Bezug zur freien Marktwirtschaft sind nicht Bestandteil dieser Arbeit. Hierzu wird auf die Literatur verwiesen (siehe Bhattacharya, Boot und Thakor 1998; Dötz 2002; vgl. Hartmann-Wendels, Pfingsten und Weber 2004, S.323ff.). Im Folgenden wird die aktuelle Rechtslage (KonTraG, KWG und die nationale Umsetzung von Basel II) zu Grunde gelegt und die quantitativen Anforderungen an die Eigenmittel sowie die qualitativen Ansprüche an die Organisation untersucht. Gegenstand der Betrachtung sind dabei ausschließlich Vorgaben, die das Management operationeller Risiken bei Kreditinstituten betreffen.

Das KonTraG wurde 1998 unter anderem mit dem Ziel in Kraft gesetzt, die Entwicklung des Risikomanagements in Unternehmen zu fördern. Diese Forderung leitet sich insbesondere aus der enthaltenen Ergänzung des Aktiengesetzes (AktG) ab, ein Überwachungssystem zur Früherkennung bestandsgefährdender Risiken zu implementieren (vgl. AktG §91 Abs.2). Das Risikomanagement umfasst nach herrschender Meinung zumindest die in Abbildung 2.3 enthaltenen Bestandteile (vgl. Gaulke 2002, S.17; Foit 2005, S.82ff.). Da jedoch das KonTraG keine spezifischen Regeln für das Management operationeller Risiken vorgibt, wird es im Weiteren nicht betrachtet.

Das Management operationeller Risiken bei Kreditinstituten ist indirekt in den Anforderungen an die Geschäftsorganisation enthalten: *„Ein Institut muss über eine ordnungsgemäße Geschäftsorganisation verfügen, die die Einhaltung der von den Instituten zu beachtenden gesetzlichen Bestimmungen gewährleistet.“* (KWG §25a Abs.1)

Hierdurch werden eine Risikostrategie, ein Kontrollsystem sowie die ausreichende Sicherheit in der Informationstechnologie gefordert. Der Paragraph stellt den Eckpfeiler der qualitativen Regulierung von Kreditinstituten auch im Kontext operationeller Risiken dar (vgl. Schneider 2005, S.583).

Entscheidender regulatorischer Rahmen für diese Arbeit ist die im November 2005 durch das Basel Committee on Banking Supervision (BCBS) festgelegte Fassung der Rahmenvereinbarung zur internationalen Konvergenz der Eigenkapitalanforderungen:

- Juli 1988: „Internationale Konvergenz der Eigenkapitalmessung und Eigenkapitalanforderungen“ (Basel I). Keine direkte Berücksichtigung operationeller Risiken.
- Januar 1996: „Änderung der Eigenkapitalvereinbarung zur Einbeziehung der Marktrisiken“ (Erweiterung Basel I).
- Juni 2004 / November 2005: „Internationale Konvergenz der Eigenkapitalmessung und der Eigenkapitalanforderungen - Überarbeitete Rahmenvereinbarung“ (Basel II). Beinhaltet erstmals operationelle Risiken.
- Oktober 2005: Verabschiedung CAD III zur EU-weiten Umsetzung (siehe CAD III; ECB 2005b).
- Dezember 2005: Verabschiedung der deutschen Mindestanforderungen an das Risikomanagement (MaRisk) (vgl. MaRisk). Die Anpassung des KWG sowie die Einführung der SolvV stehen noch aus.

Basel II beruht im Wesentlichen auf drei Säulen. Die Mindestanforderungen an das Eigenkapital (Säule I) definieren die Höhe der Eigenmittelunterlegung für Kredit,- Markt- und operationelle Risiken. Das Kontrollumfeld innerhalb der Kreditinstitute und dessen Nachvollziehbarkeit wird im aufsichtsrechtlichen Überprüfungsverfahren (Säule II) festgelegt. Hierin wird der Aufsicht ein über die reine Überwachung der Einhaltung der Vorschriften hinausgehender diskretionärer Spielraum eingeräumt. Die Regulierungsbehörde kann einschreiten, wenn das aufsichtsrechtliche Eigenkapital zwar eingehalten, jedoch aus ihrer Sicht nicht ausreichend ist. Die Marktdisziplin (Säule III) erlegt den Kreditinstituten zusätzliche Offenlegungspflichten auf. Tabelle 2.2 weist die zentralen Anforderungen an ein bankinternes Management operationeller Risiken aus:

Regelung		Forderung
Basel II Säule I	Tz.644-680	Unterlegung der Risiken mit Eigenkapital
Basel II Säule II	Tz.736+737+778	Geeignete Verfahren, aufsichtsrechtliche Überprüfung
MaRisk	AT2.2+BT1 +BTR4+AT5+AT7	Anforderungen an das Risikomanagement
Basel II Säule III	Tz.828+Tabelle 11	Nennung der Methode, Darstellung des Ansatzes
Sound Practices	S.1-14	Zuverlässiges Management operationeller Risiken

Tabelle 2.2: Regulierung operationeller Risiken

Zur Quantifizierung der operationellen Risiken und damit zur Bestimmung der aufsichtsrechtlich geforderten Eigenmittelunterlegung für operationelle Risiken (vgl. Kapitel 2.1.2) stellt Basel II drei Methoden unterschiedlicher Komplexität und Risikosensitivität zur Verfügung:

- Basisindikatoransatz
- Standardansatz
- Fortgeschrittene Messansätze (bankinterne Modelle)

In den folgenden Absätzen werden die spezifischen Anforderungen für eine Anwendbarkeit aufgezählt, eine detaillierte Beschreibung der Methoden ist hingegen Bestandteil von Kapitel 4. Die Zulassung unterschiedlich komplexer Ansätze soll zum einen die Möglichkeit zur einfachen, wenn auch vorsichtig bemessenen Abschätzung bieten, zum anderen werden durch die alternative Anwendung risikosensitiverer Ansätze Anreize zur methodischen Weiterentwicklung geschaffen (vgl. Dowd 2003, S.4). Grundsätzlich kann jedes Kreditinstitut eigenständig einen der oben genannten Ansätze wählen. Es wird jedoch von internationalen Banken erwartet, dass die Komplexität der Methode dem Umfang der Risiken angemessen ist (vgl. Basel II, Tz.647). Ein nachträglicher Wechsel zu einem einfacheren Ansatz ist darüber hinaus nicht mehr möglich.

Für die Anwendung des Basisindikatoransatzes, der das Risikopotential über den gesamten Bruttoertrag des Kreditinstitutes abschätzt, nennt Basel II keine konkreten Mindestanforderungen. Es wird jedoch darauf hingewiesen, dass zumindest die „Sound Practices for the Management and Supervision of Operational Risk“ (siehe BCBS 2003b) enthalten sein müssen (vgl. Basel II, Tz.651). Diese beschreiben in zehn Grundsätzen (z.B. Verantwortung der Geschäftsleitung oder regelmäßige Prüfung des Risikomanagements) Anforderungen an ein solides Risikomanagement. Insbesondere auch die Umsetzung des Risikomanagements über einen Prozess, hier bestehend aus Erkennung, Bewertung, Überwachung und Begrenzung der Risiken, ist Teil der Grundsätze.

Der Standardansatz (vgl. Kapitel 4.2.1) stellt durch die nach Geschäftsfeldern (vgl. Kapitel 2.2.1) differenzierte Betrachtung eine Verfeinerung des Basisindikatoransatzes dar. Um den Standardansatz anwenden zu können, müssen Kreditinstitute generell über ein bankweites Risikomanagementsystem verfügen, in das auch das oberste Verwaltungsorgan integriert ist (vgl. Basel II, Tz.660). Für internationale Kreditinstitute gilt ferner, dass das Risikomanagement klar einer organisatorischen Einheit zugewiesen wird, welche regelmäßig über die aktuelle Gefährdungslage berichtet. Zusätzlich müssen Verlustdaten je Geschäftsfeld gesammelt werden. Sämtliche Verfahren und Systeme müssen durch externe Prüfer oder die Bankenaufsicht überwacht werden (vgl. Basel II, Tz.663).

Als fortgeschrittene Messansätze (AMA) werden sämtliche bankinternen Verfahren bezeichnet, mittels derer das Kreditinstitut regulatorische Eigenkapitalanforderungen ermittelt. Diese Ansätze müssen bestimmten qualitativen und quantitativen Anforderungen gerecht werden (vgl. Basel II, Tz.666ff.). Generell gelten für die fortgeschrittenen Messansätze die gleichen qualitativen Vorgaben hinsichtlich der Organisation wie für den Standardansatz bei internationalen Kreditinstituten. Ferner sind folgende quantitative Bedingungen zu erfüllen:

- Schwerwiegende Risiken am oberen Ende einer Verteilung müssen berücksichtigt werden. Der Betrachtungszeitraum ist mit einem Jahr und das Konfidenzniveau mit 99,9% anzusetzen (vgl. Basel II, Tz.667).
- Bei der Ermittlung des Risikos ist auf die in Textziffer 644 genannte Definition abzustellen. Korrelationen können unter gewissen Rahmenbedingungen berücksichtigt werden (vgl. Basel II, Tz.669).
- Kreditinstitute müssen interne Verlustdaten entsprechend dem festgelegten Schema aus Geschäftsfeldern und Ereigniskategorien sammeln (vgl. Basel II, Tz.670ff.).
- Zur Überprüfung und Skalierung der eigenen Modelle muss das Kreditinstitut zusätzlich externe Daten hinzuziehen (vgl. Basel II, Tz.674).
- Über Szenarioanalysen soll das Kreditinstitut die Gefährdung durch schwerwiegende Ereignisse abschätzen (vgl. Basel II, Tz.675).
- Es müssen zukunftsgerichtete Faktoren des Geschäftsumfelds und des internen Kontrollsystems miteinbezogen werden (vgl. Basel II, Tz.676).

In den MaRisk sind die operationellen Risiken als wesentliche Risikokategorie enthalten (vgl. MaRisk, AT2.2). Neben den allgemeinen Vorschriften zur Risikotragfähigkeit, Risikostrategie und dem organisatorischen Aufbau sind konkrete Vorgaben zu operationellen Risiken enthalten. So ist eine Beurteilung der wesentlichen operationellen Risiken zumindest jährlich vorgesehen, hierin ist auch eine Unterrichtung der Geschäftsleitung über Art und Umfang wesentlicher Schäden enthalten. Ferner sind ausreichende Maßnahmen zur Steuerung der operationellen Risiken zu implementieren. In Bezug auf die Technologierisiken ist in den MaRisk eine klare Anforderung enthalten:

„Die IT-Systeme (Hardware- und Software-Komponenten) und die zugehörigen IT-Prozesse müssen die Integrität, die Verfügbarkeit, die Authentizität sowie die Vertraulichkeit der Daten sicherstellen.“ (MaRisk, AT7.2)

Zum Management dieser Risiken wird erwartet, dass auf gängige Standards abgestellt wird. Hierzu werden in den Erläuterungen der MaRisk das Handbuch für den IT-Grundschutz sowie der ISO 17799 Standard genannt (vgl. BaFin 2005a, S.15).

2.3 Wissensbasierte Quantifizierung

Die für das Management von Technologierisiken vorgegebenen Ziele (vgl. Kapitel 1.2, Ziele 1a - 2b) können nur insoweit gemeinsam umgesetzt werden, wie es gelingt, die Modellierung des für das Verständnis erforderlichen Wissens mit Methoden zur Quantifizierung zu kombinieren. Diese wechselseitige Beziehung ist im Risikomanagement von Kreditinstituten von entscheidender Bedeutung:

„If knowledge management is of growing importance to every kind of business, its impact is perhaps most obvious in the financial service industry. This is because effective management of knowledge is key to managing risk. And the driving issue in [...] financial services [...] today is risk.“ (Marshall, Prusak und Shpilberg 1996, S.81)

Da für diese Arbeit die Quantifizierung im Risikomanagementprozess im Vordergrund steht, wird in den folgenden Abschnitten der Zusammenhang zwischen der formalen Darstellung von Wissen und den Ansätzen zur Risikoquantifizierung untersucht. Grundlage hierfür ist die Repräsentation von Wissen mittels formaler Ontologien. Hierzu wird ein möglicher Ansatz zur Entwicklung von Ontologien dargestellt, der in Kapitel 3 seine konkrete Anwendung findet. Die in Kapitel 4 vorgeschlagene Verbindung von Wissens- und Simulationsmodellen zur Risikoquantifizierung fußt im Wesentlichen auf der Idee, Ontologien zur Repräsentation von Simulationsmodellen einzusetzen.

2.3.1 Repräsentation von Wissen

Der Begriff Wissen wird in der wissenschaftlichen Literatur aus unterschiedlichen Perspektiven betrachtet (vgl. Alavi und Leidner 2001, S.111). Für diese Arbeit stehen im Wesentlichen zwei Gesichtspunkte im Vordergrund.

Der erste beschreibt Wissen als: *„[...] the state or fact of knowing; it is understanding gained through experience or study [...]“* (Snyder and Wilson 1998, S.43). Diese auf das Verständnis bezogene Auslegung von Wissen kann zweitens über die Abgrenzung von den Begriffen Daten und Informationen erweitert werden. Der Begriff Daten bezeichnet hierbei objektive Fakten, die entsprechend syntaktischer Regeln zusammengesetzt sind. Informationen beinhalten eine Semantik und können daher vom Empfänger gezielt genutzt werden. Wissen wiederum stellt personalisierte Informationen dar, die in Bezug zu Interpretationen oder individuellen Einschätzungen stehen (vgl. Alavi und Leidner 2001, S.109).

Aufbauend auf diesen beiden Perspektiven kann Wissen ergänzend in explizites Wissen (kodifiziert) und implizites Wissen (mentales Modell) unterteilt werden (vgl. Nonaka 1994, S.16f.). Da es Ziel dieser Arbeit ist, eine Methode zur Quantifizierung operationeller Technologierisiken auf Basis eines expliziten Wissensmodells zu entwickeln, steht hier das kodifizierte Wissen im Vordergrund.

Zusätzlich zum Begriff Wissen ist auch der Begriff Wissensmanagement zu klären. Dieser bezeichnet einen systematischen Ansatz, der unter Einbeziehung von technischen und personellen Ressourcen implizites und explizites Wissen in der Organisation gezielt verwaltet und dazu nutzt, Qualitäts- und Kostenvorteile zu erzielen (vgl. Abecker und Van Elst 2004, S.435f.). Wissensmanagement kann dabei als Prozess zur Entwicklung und Generierung von Wissen oder auch als System zur Speicherung und Wiederverwendung von Wissen interpretiert werden.

Im Folgenden werden der Hintergrund formaler Ontologien im Hinblick auf die Informatik erläutert und mögliche Vorteile ihrer Verwendung, insbesondere im Kontext des Risikomanagements, aufgezeigt. Zielsetzung ist die formale kodifizierte Repräsentation von Wissen. Eine Betrachtung der philosophischen Grundlagen ist nicht Bestandteil der Arbeit. Folgende gängige Beschreibung erläutert auf abstrakte Weise die Idee formaler Ontologien:

„A conceptualization is an abstract, simplified view of the world that we wish to represent. [...] An ontology [now] is an explicit specification of [such] a conceptualization.“ (Gruber 1995, S.908)

Eine Ontologie ist in diesem Sinne ein abstraktes Modell (explicit specification), das in nachvollziehbarer und klar abgegrenzter Weise eine Begriffswelt (conceptualization) beschreibt. Formal kann eine Ontologie auch als eine logische Theorie beschrieben werden, welche die beabsichtige Bedeutung verwendeter Begriffe innerhalb einer bestimmten Konzeptualisierung erklärt (Guarino 1998, S.7).

Hieraus leitet sich das Potential von Ontologien zur Gewinnung und Modellierung von Wissen ab. Mit der Idee des „Semantic Web” (siehe Berners-Lee, Hendler und Lassila 2001) wird das Konzept auf eine technische Ebene (World Wide Web) übertragen. Folgende Definition zeigt ein in diesem Kontext gebräuchliches Verständnis:

„Ontologies have been developed to provide machine-processable semantics of information sources that can be communicated between different agents (software and humans).“ (Fensel 2004, S.3)

Zwei wichtige konzeptionelle Vorteile und Einsatzmöglichkeiten von formalen Ontologien können wie folgt beschrieben werden (vgl. Uschold und Grüninger 1996, S.7ff.):

- Der Aspekt Kommunikation bezeichnet die Fähigkeit, ein unternehmensweites oder sogar -übergreifendes, gemeinsames Verständnis der verwendeten Begriffe und Strukturen einer Domäne zu gewinnen und dieses als normatives Modell abzubilden.
- Unter Zusammenarbeit wird die Stärke von Ontologien verstanden, unterschiedliche technische Systeme oder Methoden in eine Architektur zu integrieren. Dies kann beispielsweise durch die Ermöglichung spezieller Sichten auf das abstrakte Modell des Domänenwissens erreicht werden.

Ontologien können demnach einerseits bei der Entwicklung eines präzisen Modells der Begriffe und Zusammenhänge operationeller Technologierisiken helfen. Andererseits ist es möglich, über die Entwicklung geeigneter Sichten relevante Informationen aus dem Wissensmodell in die Phase der Quantifizierung zu überführen.

Formale Ontologien können auf unterschiedliche Weise beschrieben werden, zum Beispiel mittels Frames, Description Logic (DL) oder UML (vgl. Gomez-Perez, Fernandez-Lopez und Corcho 2004, S.9ff.). In dieser Arbeit wird ausschließlich die Description Logic zur formalen Repräsentation der Technologierisiko-Ontologie verwendet.

Die DL wird allgemein als eine Familie von Sprachen zur Repräsentation von Domänenwissen in einer formalen und nachvollziehbaren Weise verstanden (vgl. Baader, Horrocks und Sattler 2004, S.4ff.). Die Bezeichnung ergibt sich zum einen daraus, dass konzeptuelle Beschreibungen (Description) verwendet werden, um die wesentlichen Artefakte der Domäne zu charakterisieren. Zum anderen geschieht dies in einer logikbasierten (Logic) Semantik. Für eine konkrete Ausprägung der DL ist dann jeweils festgelegt, welche Artefakte wie verwendet werden dürfen. Zentrale Artefakte eines in DL beschriebenen Modells sind Konzepte (verwendete Begriffe), Rollen (Beziehungen zwischen Begriffen), Restriktionen (mögliche Einschränkungen) und Individuen (konkrete Ausprägungen eines Begriffs).

Ein gewichtiger Vorteil von DL ist die Unterstützung von Inference, also die Möglichkeit neues Wissen aus bestehenden Erkenntnissen automatisch abzuleiten. Hierfür existieren Reasoning-Algorithmen, die aus den beschriebenen Konzepten und Rollen neue Zusammenhänge folgern können. Dies ist insbesondere im Rahmen der Verbindung des Modells operationeller Technologierisiken mit der Methode der Quantifizierung von Bedeutung (vgl. Kapitel 4.3; Kapitel 5.3).

Die für diese Arbeit relevanten Artefakte der DL sind Tabelle 2.3 im Überblick dargestellt. Alternativ zur Bezeichnung Rolle wird im Rahmen dieser Arbeit der geläufigere Begriff der Relation verwendet.

Artefakt	**Erläuterung**	**DL**
Universal	Menge aller möglichen Individuen einer Domäne	$\top$
Konzept	Eine bestimmte Teilmenge von Individuen	C
Äquivalenz	Zwei Konzepte beschreiben jeweils die gleichen Individuen	$C_1 \equiv C_2$
Disjunkt	Zwei Konzepte haben keine gemeinsamen Individuen	$C_1 \sqsubseteq \neg C_2$
Vererbung	Ein Konzept ist vollständig in einem anderem enthalten	$C_1 \sqsubseteq C_2$
Vereinigung	Menge der Individuen, die in min. einem Konzept enthalten sind	$C_1 \sqcup C_2$
Schnitt	Menge der Individuen, die in beiden Konzepten enthalten sind	$C_1 \sqcap C_2$
Aufzählung	Das Konzept beschreibt eine festgelegte Menge von Individuen	$C_1 \equiv \{i_1, i_2\}$
Relation	Eine Beziehung zwischen Konzepten	r
Domäne	Der Gültigkeitsbereich der Relation	$\geqslant 1\, r \sqsubseteq C_1$
Bereich	Der Wertebereich der Relation	$\top \sqsubseteq \forall r.C_2$
Attribut	Eine Eigenschaft (Mit Datentyp)	a
Domäne	Der Gültigkeitsbereich des Attributs	$\geqslant 1\, a \sqsubseteq C$
Bereich	Der Datentyp des Attributs	$\top \sqsubseteq \forall a.D$
Restriktion	Allgemeine Einschränkung der Ausprägungen einer Relation	$r.C$
Allquantor	Die Einschränkung gilt für alle Ausprägungen dieser Relation	$\forall r.C$
Existenz	Es existiert mindestens eine Ausprägung mit der Einschränkung	$\exists r.C$
Wert	Nur dieses Individuum ist zulässig	$\exists r.\{i\}$
Individuum	Ein bestimmtes Individuum	i

Tabelle 2.3: Wesentliche Artefakte
(siehe Baader, Horrocks und Sattler 2004)

Konzepte *C* im Modell stellen immer eine Menge von Individuen *i* dar. Sie können als konkrete Aufzählung einzelner Individuen oder implizit, zum Beispiel als Vereinigung ($\sqcup$) oder Schnitt ($\sqcap$) anderer Konzepte, beschrieben werden. Relationen *r* stellen Beziehungen zwischen Konzepten dar. Für diese können einschränkende Aussagen darüber getroffen werden, von welchem Konzept C_1 die Relation ausgeht ($\geqslant 1\ r \sqsubseteq C_1$) und zu welchem Konzept C_2 eine Beziehung hergestellt wird ($\top \sqsubseteq \forall\ r.C_2$). Attribute beschreiben mögliche Eigenschaften von Konzepten. Analog zur Relation kann für ein Attribut *a* festgelegt werden, zu welchem Konzept das Attribut gehört ($\geqslant 1\ a \sqsubseteq C$) sowie welcher Datentyp *D* zulässig ist ($\top \sqsubseteq \forall\ a.D$).

2.3.2 Entwicklung einer Ontologie

Für die Entwicklung von Ontologien stehen verschiedene Methodologien und Ansätze zur Verfügung (vgl. Gomez-Perez, Fernandez-Lopez und Corcho 2004, S.107ff.). Basierend auf dem IEEE Standard zur Softwareentwicklung wurde im Rahmen des METHONTOLOGY Frameworks (siehe Fernandez-Lopez, Gomez-Perez und Juristo 1997) eine übergreifende Struktur aus Aktivitäten identifiziert, die auf oberster Ebene den drei Bereichen Management, Entwicklung und Support zugeordnet werden können. Für diese Arbeit sind zunächst die Entwicklungsaktivitäten relevant.

Diese können im Kern in die Phasen Spezifikation, Konzeptualisierung, Formalisierung und Implementierung unterteilt werden:

- Durch die Spezifikation werden der Anwendungsbereich und die Domäne der zu entwickelnden Ontologie informell beschrieben. Ergebnis ist eine verbale Darstellung des beabsichtigten Modells.
- Die Konzeptualisierung strukturiert das gewonnene Wissen. Hierzu wird eine möglichst unabhängige und übersichtliche Darstellung (z.B. graphisch) gewählt, die das Modell semi-formal beschreibt.
- Die Überführung in ein formales Modell (z.B. auf Basis von DL) erfolgt in der Formalisierung.
- Während der Implementierung wird das formale Modell in eine konkrete, maschinenlesbare Darstellung (hier OWL-DL) übertragen.

Zusätzlich wird mit der Evaluation eine wichtige Supportaktivität betrachtet:

- In der Evaluation wird die Umsetzung des beabsichtigen Modells in das ontologische Modell kritisch bewertet.

In der Regel sehen konkrete Ansätze für die Ontologieentwicklung mehrere Iterationen dieser Phasen vor.

Im Folgenden werden die im Rahmen dieser Arbeit innerhalb der einzelnen Phasen eingesetzten Methoden dargestellt. Die vorgestellte Auswahl stellt einen hybriden Ansatz dar, da nicht durchgängig die Methoden eines einzelnen Ansatzes gewählt werden. Für die Auswahl der Methoden wird auf einen Vergleich zurückgegriffen, der die Abdeckung der zentralen Aktivitäten des allgemeinen Entwicklungsprozesses durch die jeweiligen Ansätze untersucht und deren Stärken und Schwächen analysiert (vgl. Gomez-Perez, Fernandez-Lopez und Corcho 2004, S.151). Zudem fließen in die Auswahl die konkreten Anforderungen an die Entwicklung der Technologierisiko-Ontologie ein. Da im Rahmen dieser

Arbeit auf die Darstellung der Iterationen verzichtet wird, ist die getroffene Einteilung in Kapitel 3 beziehungsweise Kapitel 5 nicht vollständig trennscharf im Sinne obiger Phasen.

In der Phase der **Spezifikation** (vgl. Kapitel 3.1) wird schwerpunktmäßig auf innerhalb des TOVE Projekts entwickelte Techniken zurückgegriffen (siehe Grüninger und Fox 1995). Um das Umfeld der zu entwickelnden Technologierisiko-Ontologie zu charakterisieren, werden die zentralen Hintergründe und Anforderungen prägnant in einem sogenannten Motivating Scenario zusammengefasst. In einem zweiten Schritt werden dann die konkreten Fragestellungen, die mittels der Ontologie beantwortet werden sollen, über (informelle) Competency Questions formuliert.

Die Entwicklung im engeren Sinn, also die **Konzeptualisierung** sowie die **Formalisierung** (vgl. Kapitel 3.2) erfolgt in Anlehnung an METHONTOLOGY (vgl. Gomez-Perez, Fernandez-Lopez und Corcho 2004, S.125ff.). Die Konzeptualisierung wird mittels einer unabhängigen, graphischen Darstellung (hier eigene Symbolik, angelehnt an DL) realisiert. Hierüber werden die in der Spezifikation formulierten Begriffe, ihre Hierarchie sowie die bestehenden Beziehungen charakterisiert. Auf eine detaillierte textliche Beschreibung im Sinne von METHONTOLOGY wird verzichtet. Abschließend erfolgt die Transformation der Konzeptualisierung in eine formale Sprache (hier DL).

Während der **Implementierung** wird die formal beschriebene Ontologie in eine maschinenlesbare Darstellung überführt. Hier ist es insbesondere entscheidend, dass die gewählte Sprache in der Lage ist, die im Rahmen der bisherigen Phasen entwickelten Artefakte abzubilden. Für die Implementierung von Ontologien bieten sich unterschiedliche Sprachen an (vgl. Gomez-Perez, Fernandez-Lopez und Corcho 2004, S.199ff.). In dieser Arbeit wird die auf XML/RDF(S) basierende Web Ontology Language (kurz OWL) verwendet. Eine Einführung in die OWL sowie die Darstellung der konkreten Implementierung der Technologierisiko-Ontologie erfolgen in Kapitel 5.2.

Für die **Evaluation** der Technologierisiko-Ontologie (vgl. Kapitel 3.3) wird die OntoClean-Methode (siehe Welty und Guarino 2001) zur Überprüfung der Konzepthierarchie eingesetzt. Dies erfolgt in zwei Schritten. Zuerst werden den Konzepten an die Philosophie angelehnte Meta-Eigenschaften zugewiesen:

- Die Eigenschaft der Rigidität (rigidity) drückt aus, ob das Konzept die Individuen über ihren gesamten Lebenszyklus (+R) beschreibt (z.B. *Mensch* im Gegensatz zu *Student*). Kann dies nicht unbedingt vorausgesetzt werden, ist diese Eigenschaft nicht gegeben (-R).

- Die Identität eines Konzepts beschreibt, ob die Individuen über ein bestimmtes Kriterium genau und jederzeit identifizierbar sind (+I), andernfalls gilt die Eigenschaft nicht (-I). Einen Spezialfall stellen eigene (own) Kriterien dar, die direkt vom Konzept selbst zur Verfügung gestellt werden und nicht geerbt sind (+O bzw. -O).
- Die Eigenschaft der Abhängigkeit legt fest, ob die Individuen eines Konzepts (z.B. *Eltern*) extern abhängig von der Existenz anderer Individuen eines weiteren Konzepts (z.B. *Kind*) sind (+D) oder nicht (-D).
- Als Einheit (unity) wird die Eigenschaft bezeichnet, inwieweit das Konzept ganze Individuen beschreibt. Das ist genau dann gegeben, wenn das Individuum aus der Verbindung einzelner Teile mit definierbaren Grenzen besteht (+U). Beschreibt das Konzept eher Massen (z.B. *Wasser*) gilt die Eigenschaft nicht (-U).

Mögliche Kombinationen der Eigenschaften können zu Konzeptgruppen zusammengefasst werden. Die zentrale Konzeptgruppe einer Ontologie beispielsweise ist der sogenannte Typ (+O+I+R). Solche Konzepte bilden die elementaren Bestandteile einer Ontologie. Eine Rolle (-O+I-R) beschreibt intermediäre Zustände eines Konzeptes. Kategorien (-O-I+R) stellen einen Oberbegriff einzelner Konzepte dar. Sie beschreiben häufig die Vererbungshierarchien innerhalb einer Ontologie. Attribute (-O-I-R) legen temporäre Eigenschaften eines Konzeptes fest (vgl. Welty und Guarino 2001, S.62).

In einem zweiten Schritt wird die Vererbungshierarchie daraufhin untersucht, ob die für die Meta-Eigenschaften festgelegten Regeln eingehalten werden. In Formel 2.10 sind die für diese Arbeit relevanten Regeln dargestellt. Hierbei bedeutet das Symbol → eine notwendige und der Ausdruck ¬→ eine nicht erlaubte Vererbung der Meta-Eigenschaften von Konzept ϕ nach Konzept ψ. Das Symbol ⇒ beschreibt eine notwendige Verknüpfung von Meta-Eigenschaften innerhalb eines Konzeptes.

$$\begin{array}{lll} \phi^{+I} \rightarrow \psi^{+I} & \phi^{+D} \rightarrow \psi^{+D} & \phi^{+O} \Rightarrow \phi^{+R} \\ \phi^{+U} \rightarrow \psi^{+U} & \phi^{-R} \neg \rightarrow \psi^{+R} & \phi^{+O} \Rightarrow \phi^{+I} \end{array} \qquad (2.10)$$

Falls ein Konzept über ein bestimmtes Kriterium genau und jederzeit identifizierbar ist, ein Konzept extern abhängig ist oder es immer ganze Individuen beschreibt, muss diese Meta-Eigenschaft notwendigerweise vererbt werden. Wenn ein Konzept die Individuen nicht zwangsläufig über den gesamten Lebenszyklus beschreibt, kann dieses bei abgeleiteten Konzepten nicht gefordert werden. Besitzt ein Konzept ein eigenes Kriterium, das die Individuen genau und jederzeit identifizierbar macht, so muss das Konzept die Individuen über den gesamten Lebenszyklus beschreiben.

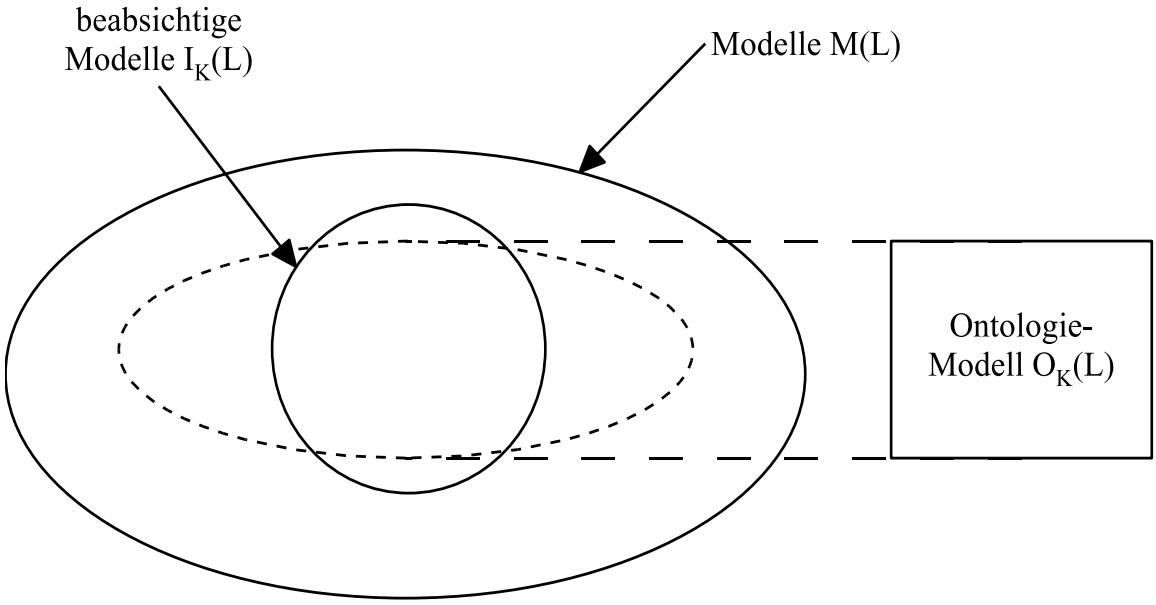

Abbildung 2.5: Ontologie-Modell
(siehe Guarino 1998; Guarino und Persidis 2003)

Abschließend werden zur Evaluation noch zwei formale Maße für die Güte einer Ontologie vorgestellt (vgl. Guarino und Persidis 2003, S.6f.). Hintergrund ist der in Abbildung 2.5 dargestellte Bezug zwischen dem Ontologie-Modell O_K und dem beabsichtigten Modell I_K im Hinblick auf die Konzeptualisierung *K*, basierend auf einer formalen Sprache *L*. Die Abdeckung (Coverage, *C*) beschreibt, zu welchem Grad die Ontologie das beabsichtigte Modell umfasst.

$$C = \frac{|I_K \cap O_K|}{|I_K|} \tag{2.11}$$

Je weniger explizit eine Ontologie beschrieben wird, desto höher ist zwangsläufig die Abdeckung. Hierbei steigt jedoch auch die Wahrscheinlichkeit, dass Konzepte zugelassen werden, die nicht im beabsichtigten Modell enthalten sind. Die Präzision (Precision, *P*) stellt daher ein Maß für den Umfang solcher nicht beabsichtigter, also falscher Aussagen in der Ontologie dar.

$$P = \frac{|I_K \cap O_K|}{|O_K|} \tag{2.12}$$

Eine optimale Ontologie verbindet eine möglichst umfassende Abdeckung bei gleichzeitig hoher Präzision.

2.3.3 Ontologien als Simulationsmodell

Zur Quantifizierung von Risiken im Finanzbereich stellen Simulationen eine häufig genutzte Alternative dar. Ein möglicher Grund ist die teilweise Nicht-Existenz analytischer Lösungen. Des Weiteren können Simulationsmodelle aber auch genutzt werden, um das Verhalten eines zu betrachtenden Systems zu analysieren. Im Rahmen dieser Arbeit wird die Simulation dazu verwendet, die Strukturen sowie die Auswirkungen von Veränderungen in der IT-Landschaft eines Kreditinstituts zu modellieren, um so mögliche Konsequenzen für die operationelle Risikosituation zu ermitteln.

In der Literatur existiert eine Vielzahl unterschiedlicher Kategorisierungen von Simulationsansätzen (siehe Nance 1993, Leemis 1996; Miller et al. 2004). Im Folgenden wird lediglich ein allgemeiner Überblick gegeben, der die Ansätze auf oberster Ebene untergliedert:

- Die Monte-Carlo-Simulation bezeichnet Ansätze, bei denen kein Bezug zur Zeit benötigt wird. Ein (nicht) zufälliges Problem wird hierbei mit Hilfe stochastischer Methoden gelöst. Kennzeichen ist das wiederholte zufällige oder auf empirischen Daten basierende Versuchen.
- Die Discrete-Event-Simulation basiert auf einer diskreten Darstellung von Zeitintervallen. Der Schwerpunkt liegt auf der Modellierung von Zustandsveränderungen. Diese können durch Ereignisse oder durch Voranschreiten der Zeit ausgelöst werden.
- Die Continuous-Simulation basiert auf stetigen Gleichungen. Hierbei erfolgt die Abbildung der Beziehung zwischen Zustand und Zeit in der Regel über eine Differentialgleichung.

Solch eine schematische Taxonomie kann grundsätzlich kritisch betrachtet werden, da in der Umsetzung aller Voraussicht nach auch hybride Ansätze Verwendung finden (siehe Fishwick 1995). Dieses Argument trifft besonders auch im Risikomanagement zu (vgl. Cuske, Dickopp und Seedorf 2005, S.80). Daher liegt der Schwerpunkt der Betrachtung mehr auf einem möglichst generischen Modell, welches den Anforderungen an eine Simulation von Technologierisiken genügt.

Ein Simulationsmodell ist allgemein ein Modell, das die für eine Simulation relevanten Konstrukte beschreibt. Dies kann in unterschiedlicher Form, beispielsweise graphisch oder mathematisch erfolgen (siehe Schmidt 1984; Garrido 2001). Für operationelle Technologierisiken sollten mindestens die zu betrachtenden Elemente, deren Abhängigkeiten und Zustände, stochastische Einfluss-

größen und finanzielle Ausgabegrößen im Modell enthalten sein. Dies kann vereinfacht auch als Input, Element und Output interpretiert werden (siehe Zeigler, Praehofer und Kim 2000).

Im Folgenden wird die Idee, formale Ontologien als Simulationsmodell zur Quantifizierung operationeller Technologierisiken einzusetzen, vorgestellt (siehe Cuske, Dickopp und Seedorf 2005) und der Begriff der Ontologie-zentrierten Simulation geprägt.

Die grundsätzliche Möglichkeit, formale Ontologien zur Darstellung von Simulationsmodellen einzusetzen, wurde auf der Winter Simulation Conference 2004 in einer eigenen Veranstaltung diskutiert (z.B. Fishwick und Miller 2004). Konkret wurde hier der Einsatz formaler Ontologien zur Verbindung des über die Anwendungsdomäne vorhandenen Wissens mit den technischen Aspekten der Simulation untersucht. Im Kontext des Semantic Web spricht man auch von einer Erweiterung der Web-basierten Simulation.

Als wesentliche Vorteile formaler Ontologien können zwei Aspekte zusammengefasst werden. Zum einen kann hierüber eine bessere Verknüpfung der auf unterschiedliche Quellsysteme verteilten Informationen erfolgen. Zum anderen verschiebt sich der Fokus von der Umsetzung technischer Details auf die eigentliche Modellierung des für die Simulation benötigten Wissens. Eine erste konkrete Anwendung ist die Entwicklung einer Ontologie für die unterschiedlichen Artefakte eines Simulationsmodells. Die Discrete-event Modelling Ontology (DeMO) beschreibt beispielsweise das technische Vokabular eines Simulationsmodells für Discrete-Event-Simulationen (siehe Miller et al. 2006).

Die konkreten Einsatzmöglichkeiten von Ontologie-Sprachen zur Modellierung von Simulationen wie beispielsweise OWL können auch aufbauend auf den bestehenden Limitationen einer rein XML-basierten Lösung analysiert werden (siehe Lacy und Gerber 2004). Ein Nachteil stellt die unzureichende Semantik von in XML beschriebenen Simulationsmodellen dar. Daher werden in diesem Zusammenhang die Möglichkeiten von OWL zur Integration von Domänenwissen untersucht. Als mögliche Anwendungsgebiete von Ontologie-Sprachen werden somit die statische Beschreibung von Domänen sowie die Unterstützung bei der Entwicklung von Simulationsmodellen gesehen.

Bisherige Ansätze, wie beispielsweise DeMO, zielen auf eine Modellierung technischer Artefakte der Simulation ab. Im Rahmen dieser Arbeit spielt jedoch vornehmlich die Modellierung fachlichen Wissens eine entscheidende Rolle. Formale Ontologien werden im Rahmen des Risikomanagements zum einen zur

Repräsentation des benötigten Fachwissens verwendet, zum anderen wird die Eigenschaft der Interoperabilität genutzt, um das modellierte Wissen mit dem technischen Simulationsmodell zu verbinden.

Um die durch Ontologien ausschließlich technisch unterstützte Simulation klar von einer bereits im Kern auf Ontologien aufbauenden Simulation abzugrenzen, wird für die vorliegende Arbeit folgende Definition geprägt:

Definition (2.4): Eine Vorgehensweise wird genau dann als Ontologie-zentrierte Simulation bezeichnet, wenn:

- die betrachtete Domäne mittels einer formalen Ontologie modelliert ist,
- daraus eine direkte automatische Transformation in ein ausführbares Simulationsmodell erfolgt
- und das Simulationsmodell zumindest aus Eingabe, Element und Ausgabe besteht.

In den folgenden Kapiteln wird nun die Umsetzung beider zentraler Ziele (vgl. Kapitel 1.2) mittels einer Ontologie-zentrierten Vorgehensweise verfolgt. Hierzu wird vor dem Hintergrund der in Kapitel 2.1 bis 2.3 dargestellten Grundlagen eine Technologierisiko-Ontologie entwickelt und die Integration in ein Simulationsmodell zur Risikoquantifizierung untersucht.

Kapitel 3
Modell operationeller Technologierisiken

Zur Umsetzung des ersten Ziels – Verständnis von Technologierisiken – ist ein formales aber flexibles Modell erforderlich, das die wesentlichen Konzepte des akzeptierten Risikoverständnisses beinhaltet und gleichzeitig Erweiterungen zulässt. Die vorgestellten Definitionen 2.1 und 2.2 allgemeiner und operationeller Risiken stellen hierfür eine Grundlage dar. Eine besondere Herausforderung liegt darin, die regulatorische Sichtweise nach Basel II mit Ansätzen der IT-Governance in Einklang zu bringen. Kernaufgabe des Modells ist es, die teils unscharfen Begriffe und Zusammenhänge innerhalb der Technologierisiken zu verbinden. Hierbei ist es ebenso wichtig, dass das Modell im Sinne der Zielsetzung relevante Aspekte des technologischen Umfelds der Bank in geeigneter Abstraktion abbildet und an strukturelle Veränderungen angepasst werden kann.

Im Folgenden wird ein Modell auf Basis einer formalen Ontologie vorgestellt. Dabei wird ein hybrider Ansatz gewählt, der die Aspekte der Ontologie-Entwicklung (vgl. Kapitel 2.3.2) in drei Phasen zusammenfasst: Zur Begriffsbildung werden das Verständnis technologischer Risiken in der Literatur spezifiziert und die existierenden Abweichungen und Widersprüche verdeutlicht. Auf dieser Basis wird zusammen mit den Grundlagen allgemeiner und operationeller Risiken eine wissensbasierte Konzeptualisierung operationeller Technologierisiken abgeleitet und als Ontologie formalisiert. Abschließend wird die Ontologie unter technischen und inhaltlichen Gesichtspunkten evaluiert.

3.1 Spezifikation der Begriffe

Das Verständnis von Technologierisiken als Teilkategorie der operationellen Risiken ist weder innerhalb des akademischen noch des bankenweiten Umfelds einheitlich geprägt. Wesentliche Ursachen hierfür sind die Unterschiedlichkeit der Hintergründe und Schwerpunkte sowie die teilweise individuelle Zielsetzung. Bereits die Vielzahl deutscher Übersetzungen des Begriffs „system risk“ aus der Basler Verordnung ist ein Indikator dieser Unschärfe: Systemrisi-

ken (vgl. Piaz 2002, S.56), IT-Risiken (vgl. Junginger, von Balduin und Krcmar 2003, S.357) oder auch Technologierisiken (vgl. Minz 2004, S.17ff.). In der Regel spiegelt der Gebrauch der Terme System, IT oder Technologie mehr eine individuelle Präferenz wider, als eine im Sinne der Informatik trennscharfe Unterscheidung darzustellen. Für diese Arbeit ist ausschließlich das inhärente Verständnis entscheidend, so dass die Bezeichnung grundsätzlich austauschbar ist. Um sprachlichen Verwirrungen vorzubeugen, wird in dieser Arbeit grundsätzlich der in der deutschsprachigen Literatur überwiegende Term Technologierisiken verwendet. In der folgenden Darstellung existierender Ansätze wird nur falls notwendig der in der Quelle verwendete Begriff angeführt.

3.1.1 Literaturüberblick

Zur Spezifikation der Technologierisiken können Ansätze aus unterschiedlichen Bereichen der wissenschaftlichen Literatur herangezogen werden (vgl. Abbildung 3.1). Für diese Arbeit liegt ein Schwerpunkt der Betrachtung auf dem regulatorischen Verständnis im Sinne von Basel II. In den diesbezüglichen Quellen werden Technologierisiken als Teilbereich der operationellen Risiken beschrieben. Darüber hinaus sind jedoch ebenso Ansätze aus dem Bereich IT-Management erforderlich, um auch die interne Risikosicht der Banken zu reflektieren. Zusätzlich bieten Richtlinien und Standards zum Thema Sicherheit in der Informationstechnologie und Umsetzung der IT-Governance Anhaltspunkte für ein Verständnis von Technologierisiken.

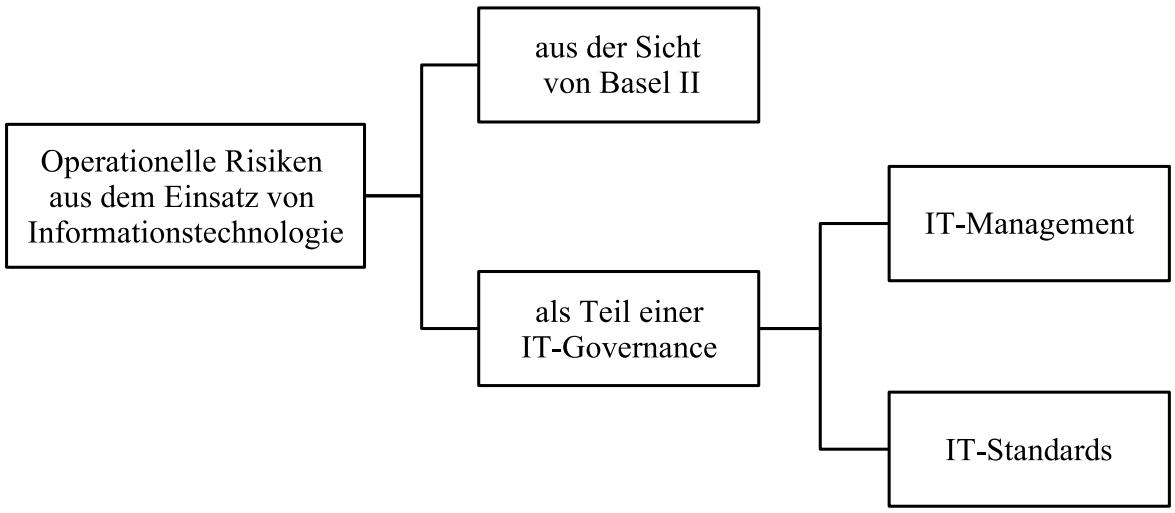

Abbildung 3.1: Darstellung existierender Ansätze

In den folgenden Abschnitten werden ausgewählte Quellen aus den unterschiedlichen Bereichen Basel II (Münchbach 2001, Röckle 2002, Van den Brink 2001, Piaz 2002, BCBS 2003b, Wolf 2005, Foit 2005), IT-Management (Krcmar 2005) sowie IT-Standards (IDW RS FAIT 1, ITGI COBIT, BSI ITGS) analysiert. Ziel des Literaturüberblicks ist ein strukturiertes Verständnis der Begriffe und Zusammenhänge von Technologierisiken.

Um Grundlagen für die Konzepte und Strukturen der Ontologie zu legen, werden die Quellen im Folgenden nicht nach ihrem thematischen Ursprung gegliedert, sondern entsprechend ihres Beitrags zum Risikoverständnis dargestellt. Hierzu können drei Klassen von Ansätzen definiert werden: exemplarische Aufzählungen, Kategorisierungen von Technologierisiken sowie Festlegung risikorelevanter Eigenschaften. Die exemplarischen Aufzählungen nennen denkbare Szenarien operationeller Technologierisiken. Sie ermöglichen ein erstes Verständnis operationeller Technologierisiken, dienen jedoch nicht direkt der Entwicklung der Ontologie. Kategorisierende Ansätze beinhalten eine weitergehende Unterteilung der vom Risiko betroffenen technologischen Ressourcen. Der Begriff der Ressource bezeichnet in diesem Kontext alle Aspekte der Informationstechnologie, die zum Betrieb der Wertkette notwendig sind (siehe Wade und Hulland 2004). Aus den unterschiedlichen Kategorisierungen wird ein wesentlicher Bestandteil der Ontologie abgeleitet, die Einteilung der Ressourcen in drei Ebenen. Abschließend wird durch die Betrachtung risikorelevanter Eigenschaften eine genauere Analyse der Risikoursachen ermöglicht. Wesentliche Eigenschaften werden in die Ontologie integriert und den Ressourcen-Ebenen zugeordnet.

3.1.2 Exemplarische Aufzählungen

Die in Kapitel 2.1.2 dargestellte Definition operationeller Risiken enthält Technologierisiken als Teilkategorie, gibt jedoch keine genauen Informationen über den weiteren Aufbau dieser Risiken. In der Literatur zu operationellen Risiken finden sich zahlreiche Aufzählungen, was unter dieser Teilkategorie zu verstehen ist. Hintergrund dieser Aufzählungen ist die Nennung möglichst vieler Aspekte und Facetten operationeller Technologierisiken, um das verantwortliche Management wirkungsvoll zu sensibilisieren. Die folgenden beispielhaften Quellen dienen als Einstieg in das Risikoverständnis dieser Arbeit und liefern einen ersten Überblick über die verwendeten Begriffe:

- Technologie als Risikoursache (siehe Münchbach 2001)
- Technische Risiken (siehe Röckle 2002)
- Beispiele für Risiken (siehe BCBS 2003b)

Nach Münchbach kann **Technologie als Risikoursache** angesehen werden. Hiernach stellen Technologierisiken Bedrohungen dar, die aus der technologischen Infrastruktur der Bank resultieren (vgl. Münchbach 2001, S.33). Das umfasst Programmier- oder Softwarefehler, eine unzureichende Kapazität von Hardware oder den Ausfall der Energieversorgung. Auch eine mangelnde Integration unterschiedlicher Anwendungssysteme, Fehler in den Schnittstellen oder Bewertungsmodellen können finanzielle Verluste induzieren. Ferner sollten nach Münchbach Gefährdungen im Bereich der physischen Sicherheit von Anlagen und Gebäuden den Technologierisiken zugerechnet werden.

Folgt man Röckle, entstehen **technische Risiken** nicht nur aus dem Einsatz von Informations- sondern auch von Kommunikationstechnologien oder der Verwendung anderer technischer Betriebsmittel (vgl. Röckle 2002, S.27f.). Als Ursachen kommen unter anderem Systemausfälle, unberechtigte Zugriffe, Probleme mit der Vernetzung oder der Kapazität der Anwendungssysteme sowie Schwächen in der Datensicherung in Frage. Exemplarisch sind hier Fehler in der Transaktionsabwicklung oder der Ausfall einer Kursversorgung zu nennen. Darüber hinaus spielen durch den Zuwachs des E-Commerce zunehmend auch Aspekte der externen Sicherheit, wie unerlaubte Systemzugriffe durch Hacker oder Computerviren, eine Rolle (vgl. Röckle 2002, S.28). Explizit ausgenommen sind Programmierfehler oder Verluste aus dem unsachgemäßen Umgang mit Betriebsmitteln. Diese sind nach Röckle der Teilkategorie Human-Risiken zuzurechnen.

Auch das Basler Komitee nennt in den „Sound Practices for the Management of Operational Risk“ **Beispiele für Risiken** aus dem Einsatz von Informationstechnologie (vgl. BCBS 2003b, S.1f.). Allgemein wird durch die Automatisierung der Prozesse das Risikopotential von manuellen Fehlern mehr zu Fehlern in Anwendungssystemen verlagert. So verursacht der Zuwachs im elektronischen Handel nicht nur zusätzliche Risiken in Form von internem oder externem Betrug sondern auch vermehrt in Form mangelnder Sicherheit der Systeme. Komplexe Unternehmensübernahmen oder Fusionen führen des Weiteren zu einem hohen technischen Integrationsaufwand bei den genutzten Anwendungssystemen, der unmittelbar mit einem gestiegenen Risiko einhergeht. Durch das wachsende Volumen der elektronisch bearbeiteten Transaktionen kommt zudem der Verfügbarkeit der Anwendungssysteme eine besondere Bedeutung zu.

Zusammengefasst beinhalten die in diesem Abschnitt dargestellten exemplarischen Aufzählungen reale Szenarien, wie zum Beispiel Fehler in der elektronischen Verarbeitung von Transaktionen oder Risiken aus der Integration heterogener Systeme. Über diese Beispiele werden indirekt die von Technologierisiken betroffenen Bereiche sowie die verursachenden Elemente aus dem technologischen Umfeld der Bank aufgezählt. Hierunter fallen unter anderem techni-

sche Ressourcen wie Hardware, Software oder Infrastruktur. Ferner wird auf die besondere Bedeutung komplexer Anwendungssysteme für die Unterstützung der Wertkette hingewiesen. Für sämtliche Ressourcen ist die Aufrechterhaltung risikorelevanter Eigenschaften wie Sicherheit oder Verfügbarkeit entscheidend.

Die exemplarischen Aufzählungen sind grundsätzlich geeignet, ein einleitendes Verständnis operationeller Technologierisiken und verwendeter Konzepte zu schaffen und diese oberflächlich von anderen Risikokategorien abzugrenzen. Ferner werden relevante Aspekte und Ziele des Risikomanagements anschaulich zusammengefasst. Entscheidend ist, dass über Bedrohungsszenarien eine klare Motivation für das Management von Technologierisiken gegeben wird.

Für die Entwicklung eines Modells der Technologierisiken können Aufzählungen jedoch ausschließlich als Grundlage dienen. Das Fehlen einer präzisen Klassifizierung der Risiken und der verursachenden Ressourcen erschwert die Bildung eines formal definierten Modells. Weiterhin werden die Begriffe nicht klar und überschneidungsfrei benutzt. So ist die Differenzierung zwischen Software und System nicht eindeutig. Elementar für ein Ontologie-zentriertes Modell sind jedoch eine klare Taxonomie der Begriffe wie der technologischen Ressourcen und der risikorelevanten Eigenschaften. Ferner ist eine möglichst umfassende Aufzählung der Bedrohungen und Aspekte ohne weitere Struktur kaum möglich (vgl. Piaz 2002, S.56).

3.1.3 Kategorisierung technologischer Risiken

Auf der Grundlage der Aufzählungen möglicher Risikoszenarien müssen die darin angedeuteten Strukturen weiter herausgearbeitet und die verwendete Begriffshierarchie präzise spezifiziert werden. Um die zielgerichtete Analyse und Modellierung operationeller Technologierisiken in Form einer Ontologie zu unterstützen, werden die betroffenen Bereiche sowie die verursachenden Ressourcen weiter untergliedert. Hierdurch wird die Ursächlichkeit der Risiken hervorgehoben und das Verständnis gefördert. In der Literatur existieren unterschiedliche begriffliche Unterteilungen der Technologierisiken, die jeweils eine Kategorisierung nach fachlichen oder technischen Kriterien vornehmen.

- Risiken aus Informationssystemen (siehe Van den Brink 2001)
- Systemrisiken als eine Art operationeller Risiken (siehe Piaz 2002)
- Risikobegriff im IT-Risk Management (siehe Krcmar 2005)
- Information System Risks (siehe Wolf 2005)
- Systemrisiken als Kategorie operationeller Risiken (siehe Foit 2005)

Die Unterteilung der **Risiken aus Informationssystemen** kann nach dem Grad ihrer Integration in die Wertschöpfungskette erfolgen. Dabei wird zwischen allgemeinen, anwendungsbezogenen und anwenderbezogenen Risiken differenziert (vgl. Van den Brink 2001, S.7). Die allgemeinen Risiken beziehen sich auf die grundlegende Informationstechnologie einer Bank und haben nur einen indirekten Bezug zur Wertkette. Darunter sind zum Beispiel unberechtigte interne oder externe Zugriffe sowie ein unzureichendes Change-Management zu verstehen. Auch das Capacity-Management, Maßnahmen zur Notfallplanung sowie ausreichende Verfahren zur Datensicherung beeinflussen die allgemeinen Risiken. Die anwendungsbezogenen Risiken betreffen unmittelbar die Verarbeitung der Informationen im Rahmen des Bankbetriebs. Aufgrund von Fehlern in den Abläufen werden die Daten der Bank falsch oder verspätet verarbeitet. Auch eine lückenhafte Datengrundlage, die zu einem nicht vollständigen Ergebnis führt, ist vorstellbar (vgl. Van den Brink 2001, S.10). Die anwenderbezogenen Risiken entstehen an der Schnittstelle zwischen Mensch und Computer. Bewusste oder unbewusste Fehler bei der Benutzung von Informationssystemen führen zu finanziellen Verlusten. Dieser Teil ist jedoch nicht frei von Überschneidungen mit den operationellen Risiken aus menschlichem Versagen.

Die **Systemrisiken als eine Art operationeller Risiken** stellen neben dem menschlichen Versagen und den Prozessrisiken einen Kernbestandteil der operationellen Risiken dar. Sie können nach Piaz in Hardwarerisiken, Softwarerisiken, Datenrisiken und Modellrisiken untergliedert werden (vgl. Piaz 2002, S.56). Während Hardwarerisiken sich auf den Ausfall physischer Komponenten beziehen, beschreiben Softwarerisiken Probleme in der Kommunikation oder Kompatibilität von Programmen. Risiken in der Datenqualität oder den Netzwerken werden unter dem Begriff Datenrisiken zusammengefasst. Fehler in den Anwendungen selbst werden als Modellrisiken bezeichnet. Entscheidend für die Zusammenführung der einzelnen Risikotypen zu den Systemrisiken ist das zugrunde liegende Verständnis von Systemen. Hiernach besteht ein System aus der Gesamtheit einzelner Elemente. Im Sinne dieses Verständnisses von Systemrisiken ist ein System demnach gleichzusetzen mit der Kombination aus Hardware, Software, Daten und Modellen (vgl. Piaz 2002, S.58).

Durch die steigende Bedeutung des Einsatzes von Informationssystemen zur Unterstützung der Geschäftsprozesse, ist das IT-Risk Management als wesentlicher Bestandteil eines ganzheitlichen Risikomanagements zu betrachten (vgl. Krcmar 2005, S.439). Nach Krcmar beinhaltet der **Risikobegriff im IT-Risk Management** die unzureichende Unterstützung der zentralen Geschäftsprozesse durch IT. Diese Unterstützungsfunktion umfasst den gesamten Lebenszyklus und erlaubt eine Unterteilung in folgende Bereiche: Die Sicherstellung einer funktionstüchtigen Infrastruktur, den sicheren Betrieb der Systeme, die termin-

und bedarfsgerechte Fertigstellung von IT-Projekten und die Festlegung einer geeigneten IT-Strategie. Als Risiken aus der Infrastruktur werden unter anderem die unzureichende Verfügbarkeit oder Sicherheit der genutzten Informationstechnologie eingeordnet. Der sichere Betrieb der Informationssysteme betrifft direkt die unterstützten Geschäftsprozesse, da Störungen im Systembetrieb zu Disfunktionalitäten in den Prozessen führen. Ursachen für Risiken aus IT-Projekten sind beispielsweise nicht eingehaltene Termine, überschrittene Budgets oder eine unzureichende Qualität. Eine mangelnde Strategieorientierung oder fehlerhafte Entscheidungen sind den Risiken aus IT-Strategien zuzurechnen. Das letzte Risikofeld geht jedoch über das Basler Verständnis operationeller Risiken hinaus. Als wichtiger Punkt ist festzustellen, dass die beschriebenen Risiken nicht unabhängig sind, sondern Interdependenzen aufweisen (vgl. Krcmar 2005, S.440). So kann die Verfügbarkeit von Technologie den Betrieb der Systeme stören oder ein kritisches Projekt die gesamte IT-Landschaft beeinflussen.

Einem umfassenderen Verständnis des Informationssystems folgt Wolf, wonach das Informationssystem sowohl das rein technische System (IT), wie Hardware oder Software, als auch organisatorische, prozessuale oder personelle Aspekte enthält (vgl. Wolf 2005, S.13). Folglich ist die Informationstechnologie nur ein Teil des Informationssystems. Konsequenterweise beinhalten die **Information System Risks** neben möglichen Verlusten aus dem Ausfall von IT, auch Schwächen in IT-gestützten Prozessen, Fehler von IT-Mitarbeitern oder externe Ereignisse mit Bezug zur IT. Darunter sind unter anderem Angriffe auf die Sicherheit der IT, Zugriffe durch nicht autorisiertes Personal oder Know-How-Verluste zu verstehen. Nach diesem weiten Verständnis stellen die Risiken aus Informationssystemen einen Querschnitt aus dem gesamten Spektrum operationeller Risiken dar (vgl. Wolf 2005, S.56). Durch diese ausgedehnte Betrachtung sollen alle Risiken, die aus der Verbindung von Informationssystemen und dem Betrieb der Geschäftsprozesse resultieren, berücksichtigt werden.

Auch für Foit stellen die **Systemrisiken als Kategorie operationeller Risiken** den Ausgangspunkt für eine weitere Systematisierung dar (vgl. Foit 2005, S.33ff.). Diese umfassen sämtliche Risiken aus dem Bereich Technologie. Eine weitere Unterteilung erfolgt hier entsprechend den Funktionsbereichen in Anlehnung an den technologischen Lebenszyklus. Risiken aus der Entwicklung werden den Projektrisiken zugewiesen. Aus dem Betreiben sowie der Überwachung der technologischen Lösungen resultieren die Betriebsrisiken. Hierunter sind unter anderem Ausfälle oder Verarbeitungsfehler zu subsumieren. Aspekte der Sicherheit im technologischen Umfeld werden bei Foit 2005 den Security-

Risiken zugeordnet. Eine besondere Betrachtung erfährt das Thema IT-Outsourcing. Aufgrund der hervorgehobenen Bedeutung werden damit einhergehende Risiken gesondert unter dem Begriff Outsourcing-Risiken betrachtet.

Die dargestellten Kategorisierungen lassen sich trotz abweichender Auffassungen verbinden, da sie über zumindest eine inhaltliche Gemeinsamkeit verfügen. Die verursachenden oder betroffenen Ressourcen können in drei Ebenen unterschiedlicher fachlicher Ausprägung zusammengefasst werden. Grundlage der Technologierisiken sind erstens elementare Komponenten der Informationstechnologie. Diese stellen die technische Basis der Informationsverarbeitung im Rahmen der Geschäftsprozesse dar. Darunter sind Hardware, Software, Netzwerke sowie die allgemeine IT-Infrastruktur zusammenzufassen. Darauf aufbauend kann zweitens ein Informations- oder Anwendungssystem als Komposition von IT-Komponenten aufgefasst werden, das die Verarbeitung von Informationen durch die Geschäftsprozesse unterstützt. Zusätzlich sind drittens Maßnahmen, die im Rahmen des Systemlebenszyklus durchgeführt werden, in eine ganzheitliche Risikobetrachtung zu integrieren. Hierzu zählen Projekte zur Einführung, Umstellung oder Ablösung eines Systems sowie Aufgaben des Regelbetriebs. Ergänzend zu den unterschiedlichen Ebenen sind die Interdependenzen zwischen den einzelnen Ebenen zu erfassen.

Die dargestellten Kategorisierungen der Technologierisiken über eine Einteilung der technologischen Ressourcen ist wesentlich, um den Umfang der Risiken vollständig zu begreifen. Über die Bildung von Kategorien ist es möglich, eine Abgrenzung vorzunehmen, was Bestandteil der Technologierisiken ist und was bewusst ausgeschlossen wird. Entscheidend ist, dass durch die Einteilung der technologischen Ressourcen ein erster Bezug zum Hintergrund der Risiken gegeben ist und so im Gegensatz zu den exemplarischen Aufzählungen die Ursächlichkeit strukturiert hervorgehoben wird.

In Bezug auf die Bildung von Kategorien kann angemerkt werden, dass die in der Literatur getroffenen Einteilungen nicht widerspruchsfrei sind. Weder die verwendeten Begriffe, noch die getroffene Unterscheidung oder Abgrenzung ist eindeutig. Für ein einheitliches Verständnis müssen jedoch mögliche Widersprüche und Überschneidungen vermieden werden. Ferner muss das zu entwickelnde Verständnis von Technologierisiken einerseits in Einklang mit Basel II gebracht werden, was insbesondere im Hinblick auf eine zu weite Auslegung der Technologierisiken kritisch erscheint. Andererseits müssen Konzepte aus der IT-Governance in das Modell der Technologierisiken einfließen. Abschließend sagt eine Kategorisierung der Risiken nicht direkt etwas über die Auslöser der Verluste aus. Die bisher angedeuteten risikorelevanten Eigenschaften, wie Verfügbarkeit oder Sicherheit, müssen daher detailliert beschrieben und den einzelnen Kategorien zugeordnet werden.

3.1.4 Risikorelevante Eigenschaften

Infolge der wachsenden Bedeutung von Informationstechnologie für Unternehmen entstehen Richtlinien, Standards und Anforderungen an Qualität und Vorgehensweise, die Ziele für einen sicheren und ordnungsmäßigen Einsatz von IT definieren. Ergänzend zu den oben dargestellten Aufzählungen und Kategorisierungen operationeller Technologierisiken werden hier normative Ansätze zur Sicherheit und Ordnungsmäßigkeit analysiert. Hieraus sind für die wesentlichen technologischen Ressourcen risikorelevante Eigenschaften ableitbar. Um der regulatorischen und der betriebswirtschaftlichen Sichtweise Rechnung zu tragen, werden sowohl nationale Standards mit Bezug zur Rechnungslegung, technische Leitfäden als auch Vorgaben zur Verlässlichkeit von Projekten und Prozessen betrachtet. Dies wird durch internationale Anforderungen an das Management der Informationstechnologie ergänzt.

- Ordnungsmäßige Buchführung bei Einsatz von Informationstechnologie (siehe IDW RS FAIT 1)
- IT-Grundschutz (siehe BSI ITGS)
- Control Objectives for Information and related Technology (siehe ITGI COBIT)

Unternehmen tragen bei der Erreichung ihrer Ziele die Verantwortung für die Einhaltung gesetzlicher Vorschriften in der Rechnungslegung. Das gilt in gleicher Weise, wenn dazu Informationstechnologie eingesetzt wird. Hierfür definiert das Institut der Wirtschaftsprüfer (IDW) einen Standard zur **ordnungsmäßigen Buchführung bei Einsatz von Informationstechnologie**. Grundlage ist der Begriff des sogenannten IT-Systems, welches aus den Elementen IT-gestützte Geschäftsprozesse, IT-Anwendungen und IT-Infrastruktur besteht. Zusätzlich wird das IT-System durch die IT-Organisation sowie das IT-Umfeld ergänzt und mittels des IT-Kontrollsystems überwacht. Hierfür definiert das IDW Anforderungen an die Sicherheit: Es werden Vertraulichkeit (ausschließlich berechtigte Weitergabe), Integrität (inhaltliche Korrektheit), Verfügbarkeit (Erfüllbarkeit vorgesehener Aufgaben), Autorisierung (berechtigter Zugriff), Authentizität (Zuordnung zum Verursacher) und Verbindlichkeit (Einhaltung der Vorschriften) genannt. Diese Eigenschaften sind die Voraussetzung für den ordnungsmäßigen Betrieb der Informationstechnik und damit der Verlässlichkeit der Informationen in der Rechnungslegung (vgl. IDW RS FAIT 1, Tz.20). Zusätzlich müssen bei der IT-gestützten Rechnungslegung die Kriterien der Ordnungsmäßigkeit eingehalten werden: Vollständigkeit (lückenlose Erfassung der Geschäftsvorfälle), Richtigkeit (inhaltlich zutreffende Abbildung), Zeitgerechtheit (korrekte Buchungsperiode), Ordnung (Erfassung nach Zeit und Konten), Nachvollziehbarkeit (Verständlichkeit für sachverständigen Dritten),

Unveränderlichkeit (Nachvollziehbarkeit der Änderungen). Ausdrücklich weist das IDW noch auf Risiken aus Veränderungen, wie beispielsweise der Entwicklung, Einführung oder Ablösung von Systemen, hin (vgl. IDW PS 330, Tz.18).

Aufgrund des zunehmenden Einsatzes von Informationstechnik sowohl in der öffentlichen Verwaltung als auch in der Wirtschaft, steigt die Abhängigkeit von der Funktionstüchtigkeit der genutzten IT (vgl. BSI ITGS, S.10). Ein sicherer und ordnungsmäßiger Betrieb ist in vielen Fällen eine Voraussetzung für das Erreichen der unternehmerischen Ziele. Aus diesem Grund stellt das Bundesamt für Sicherheit in der Informationstechnik (BSI) ein umfangreiches Handbuch für den **IT-Grundschutz** (ITGS) zur Verfügung. Auch hierin werden Verfügbarkeit, Vertraulichkeit und Integrität als wesentliche Sicherheitsziele festgelegt. Im Rahmen des Handbuchs werden konkrete Gefährdungspotentiale für die einzelnen Komponenten der Informationstechnik und Informationsverarbeitung entworfen und zu treffende Gegenmaßnahmen dargestellt. Diese Komponenten werden zu den Bausteinen übergeordnete Komponenten, Infrastruktur, nicht vernetzte Systeme, vernetzte Systeme, Datenübertragungseinrichtungen, Telekommunikation und sonstige IT-Komponenten zusammengefasst. Die Gefährdungspotentiale werden in die Gruppen höhere Gewalt, organisatorische Mängel, menschliche Fehlhandlungen, technisches Versagen und vorsätzliche Handlungen unterteilt (vgl. BSI ITGS, S.18). Der Fokus des IT-Grundschutzhandbuchs ist eine möglichst umfassende Darstellung der technischen Bedrohungen und Gegenmaßnahmen im Umfeld der Unternehmens-IT. Diese kann verwendet werden, um im Rahmen eines Audits die Strukturen zu untersuchen und zu verbessern. Gleichzeitig sind die Sicherheitsanforderungen jedoch auch frühzeitig bei Projekten, wie der Planung eines neuen Netzes oder Neuanschaffungen von IT-Systemen, zu berücksichtigen (vgl. BSI 2005, S.18).

„For many organisations, information and the technology that supports it represent the organisation's most valuable assets“ (ITGI COBIT, S.5). Daher wird dem Management der Technologierisiken eine hohe Bedeutung beigemessen. Das IT Governance Institute veröffentlicht die **Control Objectives for Information and Related Technology** (COBIT), um einen unterstützenden Leitfaden für das Management, Anwender und IT-Prüfer zur Verfügung zu stellen. Der Standard enthält konkrete Managementrichtlinien, Kontrollziele und Prüfungsleitfäden. Zentraler Baustein sind jedoch die Kontrollziele, die für die wesentlichen IT-Prozesse definiert werden. Dabei werden die IT-Prozesse in die Kategorien Planung und Organisation, Beschaffung und Implementierung, Auslieferung und Support sowie Überwachung unterteilt. Die IT-Prozesse dienen dem Betrieb sowie der Steuerung der zentralen IT-Ressourcen, die gemeinsam mit den IT-Prozessen die für die Erreichung der Geschäftsziele benötigten Informationen zur Verfügung stellen. Unter den IT-Ressourcen werden in COBIT

Daten, Anwendungssysteme, Technologie, Infrastruktur sowie Humankapital verstanden. Als Maßstab für die Verarbeitung der Informationen des Unternehmens werden die risikorelevanten Eigenschaften Effektivität, Effizienz, Vertraulichkeit, Integrität, Verfügbarkeit, Zuverlässigkeit und Compliance definiert (vgl. ITGI COBIT, S.14). Der Standard legt nun mittels der Kontrollziele für jeden IT-Prozess den Einfluss auf diese Kriterien fest und stellt einen Bezug zu den betroffenen IT-Ressourcen her. So wird über die Erfüllung der Kontrollziele sichergestellt, dass die IT-Ressourcen keinen negativen Einfluss auf die Informationskriterien haben.

Zusammenfassend werden zwei entscheidende Aspekte der in diesem Abschnitt erläuterten Eigenschaften festgehalten. Erstens wird in der Regel das zugrunde liegende Verständnis der Technologierisiken klar spezifiziert. Zweitens stellen relevante Eigenschaften der Sicherheit, Ordnungsmäßigkeit oder Zuverlässigkeit einen Eckpfeiler der dargestellten Quellen dar. Mittels dieser Eigenschaften können die Anforderungen an IT-Komponenten, Anwendungssysteme und Aufgaben des IT-Managements berücksichtigt werden. Ziel ist es, durch die Sicherstellung der Eigenschaften, die mit dem Einsatz von Informationstechnologie verbundenen Risiken zu reduzieren. Wichtig sind für IT-Komponenten häufig Kriterien der IT-Sicherheit, wie beispielsweise Integrität oder Verfügbarkeit. Für die Anwendungssysteme rücken eher die Eigenschaften der Ordnungsmäßigkeit, wie Richtigkeit oder Vollständigkeit in den Vordergrund. Für die Zuverlässigkeit der Vorhaben im Rahmen des Systemlebenszyklus, hier insbesondere Aufgaben des Betriebs oder interne Projekte, sind besonders die Ziele Effizienz und Effektivität relevant.

Die für Technologierisiken relevanten Eigenschaften der technologischen Ressourcen sind wichtiger Bestandteil des Risikoverständnisses. So kann nicht nur deren Umfang, sondern auch die Art der Bedrohung genauer analysiert werden, welche sich in nicht ausreichender Sicherheit, Ordnungsmäßigkeit oder Zuverlässigkeit manifestiert.

Analog zur Vielzahl der existierenden Kategorisierungen wird der Umfang und Inhalt der Eigenschaften in den dargestellten Quellen uneinheitlich aufgefasst und keine klare Begrifflichkeit verwendet. Weiterhin passt die gewählte Einteilung der Eigenschaften auch nicht in jedem Fall zu den in Kapitel 3.1.3 festgelegten Ressourcen-Ebenen. Zudem ist die Zuordnung der risikorelevanten Eigenschaften im Hinblick auf Basel II nicht unkritisch. Wichtig ist es daher, auch für die Eigenschaften ein möglichst umfassendes, aber auf jeden Fall explizites Modell zu formulieren und dieses mit der Einteilung in Ebenen zu verbinden.

3.1.5 Kritischer Vergleich

Zur Entwicklung einer Technologierisiko-Ontologie müssen die spezifizierten Kategorisierungen und risikorelevanten Eigenschaften vor dem Hintergrund der exemplarischen Aufzählungen verglichen und auf Basis der Gemeinsamkeiten zusammengeführt werden. Daneben sind die durch Basel II vorgegebenen Abgrenzungen zu berücksichtigen. Da die Aufzählungen keinen formalen Charakter haben, sind sie von der folgenden Synopse ausgenommen. Sie spielen jedoch für die anschließende Entwicklung der Competency Questions eine wichtige Rolle. In Tabelle 3.1 werden die Ressourcen der unterschiedlichen Kategorisierungen in drei Ebenen gruppiert: Atomare **IT-Komponenten**, komplexe **Anwendungssysteme** mit besonderer Bedeutung im Rahmen der Wertschöpfung und **IT-Managementaufgaben**. Diese Einteilung entspricht im Kern auch der Auffassung der MaRisk (vgl. MaRisk, AT7.2; Kapitel 2.2.4). Über das Verständnis von Basel II hinausgehende technologische Ressourcen werden separat ausgewiesen. Falls die Einteilung nicht überschneidungsfrei möglich ist, werden die Ressourcen mehreren Ebenen zugeordnet.

<table>
<tr><th rowspan="2">Ansatz</th><th colspan="3">Ebenen technologischer Ressourcen</th><th rowspan="2">Über Basel II hinausgehend</th></tr>
<tr><th>IT-Komponenten</th><th>Anwendungssysteme</th><th>IT-Managementaufgaben</th></tr>
<tr><td>Van den Brink 2001</td><td>allgemeine Risiken</td><td>anwendungsbezogene Risiken</td><td>–</td><td>anwenderbezogene Risiken</td></tr>
<tr><td>Piaz 2002</td><td colspan="2">Hardware-, Software-, Daten- und Modellrisiken</td><td>–</td><td>–</td></tr>
<tr><td>Krcmar 2005</td><td>Risiken aus Infrastruktur</td><td colspan="2">Risiken aus Systembetrieb, Risiken aus IT-Projekten</td><td>IT-Strategierisiken</td></tr>
<tr><td>Wolf 2005</td><td colspan="2">Risiken aus Technischem System (IT)</td><td colspan="2">IT-Prozessrisiken, IT-Mitarbeiter-Risiken, externe IT-Risiken</td></tr>
<tr><td>Foit 2005</td><td>Security-Risiken</td><td>Betriebsrisiken</td><td>Projektrisiken</td><td>Outsourcing</td></tr>
</table>

Tabelle 3.1: Verdichtung Risikokategorien zu Ebenen

Im Rahmen dieser Arbeit werden die technologischen Ressourcen in IT-Komponenten, Anwendungssysteme und IT-Managementaufgaben unterteilt. Diese Einteilung ist nicht als abgeschlossen zu verstehen, sie verkörpert vielmehr die Grundlage für ein belastbares Risikoverständnis. Auf dieser Basis ist es möglich, ein Ontologie-zentriertes Modell von Technologierisiken zu entwickeln, das sowohl formal spezifiziert als auch erweiterbar ist. Auf die Einführung einer

finalen Definition wird in diesem Zusammenhang bewusst verzichtet. Zwischen den drei Ebenen existieren unterschiedliche Wirkungszusammenhänge. IT-Komponenten formen die übergeordneten Anwendungssysteme, die in gegenseitiger Abhängigkeit stehen. IT-Managementaufgaben haben ebenfalls Einfluss auf die Anwendungssysteme. Da weitergehende Aspekte wie IT-Strategien im operationellen Risikoverständnis gemäß Basel II ausgeschlossen werden, sind diese hier nicht Bestandteil der Technologierisiken. Ferner sind Risiken, die mit den Benutzern oder den unterstützten Prozessen verbunden sind, mehr den jeweiligen Teilkategorien Human und Prozess zuzuordnen.

Die aufgeführten risikorelevanten Eigenschaften müssen nun den festgelegten Ebenen zugewiesen werden. Tabelle 3.2 zeigt eine entsprechend der Ebenen festgelegte Gruppierung der in den Quellen aufgeführten Eigenschaften.

Ansatz	**Risikorelevante Eigenschaften der Ebenen**		
	Sicherheit der IT-Komponenten	**Ordnungsmäßigkeit der Anwendungssysteme**	**Zuverlässigkeit der IT-Management-aufgaben**
IDW RS FAIT 1	Vertraulichkeit, Integrität, Verfügbarkeit, Autorisierung, Authentizität, Verbindlichkeit	Vollständigkeit, Richtigkeit, Zeitgerechtheit, Ordnung, Nachvollziehbarkeit, Unveränderlichkeit	–
BSI ITGS	Verfügbarkeit, Vertraulichkeit, Integrität	–	–
ITGI COBIT	Vertraulichkeit, Integrität, Verfügbarkeit	Zuverlässigkeit, Compliance	Effektivität, Effizienz

Tabelle 3.2: Zuordnung risikorelevante Eigenschaften zu Ebenen

Die obigen Eigenschaften decken in unterschiedlicher Tiefe und Breite die technologischen Ressourcen ab. Ferner sind die Quellen nicht überschneidungsfrei definiert. Im Rahmen dieser Arbeit wird deshalb eine aggregierende Sichtweise eingenommen. Die Kriterien der Sicherheit werden auf Integrität, Vertraulichkeit und Verfügbarkeit eingeschränkt, die Ordnungsmäßigkeit als Vollständigkeit, Zeitgerechtheit und Richtigkeit interpretiert sowie die Zuverlässigkeit der IT-Managementaufgaben als Effektivität und Effizienz festgelegt. Weder die Einteilung der Ressourcen in die drei Ebenen noch die Auswahl der Eigenschaften tragen einen endgültig definierenden Charakter. Da beides einer individuellen Sichtweise entspricht, müssen grundsätzlich Anpassungen oder Erweiterun-

gen möglich sein. An dieser Stelle zeigt sich ein wesentlicher Vorteil der Modellbildung mittels formaler Ontologien. Das Verständnis wird explizit formalisiert ohne jedoch über eine starre Definition abschließend festgelegt zu sein.

Ergebnis der Spezifikationsphase ist ein Motivating Scenario, das die Anforderung an die Ontologie-Entwicklung zusammenfasst (vgl. Grüninger und Fox 1995, S.2): Gewinnung eines bankinternen und aufsichtsrechtlich akzeptierten Verständnisses von Technologierisiken, das sich konsistent in das Management operationeller Risiken integriert. Die Competency Questions Q1 bis Q3.3 verfeinern die Anforderungen an die zu entwickelnde Ontologie. Die erste Frage Q1 bezieht sich auf die Notwendigkeit, das Verständnis von Technologierisiken in den allgemeinen Risikobegriff insbesondere vor dem Hintergrund der Quantifizierung einzubetten. Die Fragen Q2.1 bis Q3.1 betreffen die Betrachtung der Technologierisiken als Teilkategorie der operationellen Risiken bei Banken. Die Fragen Q3.2 und Q3.3 leiten sich direkt aus der in den vorangegangenen Abschnitten dargestellten Literatur zu Technologierisiken ab.

Q1: Welches Modell allgemeiner Geschäftsrisiken kann als Grundlage für das Verständnis von Technologierisiken verwendet werden?

Q2.1: Wie kann dieses Risikoverständnis auf operationelle Risiken, hier wesentlich nach Basel II, verengt werden?

Q2.2: Wie ist der Bezug zur Wertschöpfung der Bank und welche möglichen finanziellen Effekte müssen berücksichtigt werden?

Q3.1: Wie kann das Modell der Technologierisiken in das Verständnis nach Basel II integriert werden? Welche Ansätze aus der IT-Governance sollen dabei berücksichtigt werden?

Q3.2: Welche Ressourcen gibt es im Bereich operationeller Technologierisiken? Wie können diese kategorisiert werden?

Q3.3: Was sind die zentralen risikorelevanten Eigenschaften?

3.2 Entwicklung der Ontologie

Die Fragen Q1 bis Q3.3 geben die weitere Vorgehensweise für die Entwicklung der Technologierisiko-Ontologie vor. Zuerst setzt eine solche Ontologie ein grundlegendes Verständnis allgemeiner Geschäftsrisiken voraus. Anschließend muss dieses auf die Begriffswelt der operationellen Risiken bei Banken verdichtet werden. Im letzten Schritt wird das Modell der Technologierisiken aus den in der Spezifikationsphase (vgl. Kapitel 3.1) beschriebenen Ansätzen abgeleitet und in das Verständnis operationeller Risiken eingebettet. Die Beschreibung der Konzepte erfolgt hierbei formal in Description Logic (vgl. Kapitel 2.3.1).

3.2.1 Allgemeine Geschäftsrisiken als Grundlage

Grundlage der Technologierisiko-Ontologie ist eine aussagekräftige und klar abgegrenzte Begriffswelt der allgemeinen Geschäftsrisiken. Wie bereits in Kapitel 2.1.1 dargestellt, existiert in der wissenschaftlichen Literatur hierzu kein vollständig einheitliches Verständnis. Die Konzeptualisierung wird entsprechend den dort vorgestellten Ansätzen vorgenommen und fußt auf der im Rahmen dieser Arbeit verwendeten Definition 2.1.

Nach dem extensiven Verständnis ist das Geschäftsrisiko unteilbar mit jedwedem Prozess der unternehmerischen Leistungserstellung verbunden. Zur genaueren Betrachtung der Risiken wird die Leistungserstellung als Wertkette (*ValueChain*), zusammengesetzt aus (*compose*) verschiedenen Aktivitäten (*Activity*), dargestellt (vgl. Porter 2000, S.66ff.).

$$ValueChain \equiv \exists\, compose\,.\,Activity \tag{3.1}$$

Eine direkte Definition des Risikobegriffs ist jedoch nicht Bestandteil des extensiven Risikoverständnisses. Daher wird die Betrachtung um die Ursachenbezogene Sichtweise erweitert. Hiernach resultiert Risiko aus einer ungenauen Informationslage über zukünftige Szenarien zum Zeitpunkt der Entscheidungsfindung. Der Grad der Information wird disjunkt in die drei Zustände (vgl. Abbildung 2.1) vollständig bekannt (*certainty*), Eintrittswahrscheinlichkeiten bekannt (*probability*) und vollständig unbekannt (*uncertainty*) unterteilt.

$$Information \equiv \{\, certainty\,,\ probability\,,\ uncertainty\,\} \tag{3.2}$$

Informationen über Eintrittswahrscheinlichkeiten werden als stochastische Verteilungen abgebildet (vgl. Braun 1984, S.24ff.). Als Risiko wird eine möglicherweise ungünstige Entscheidung interpretiert, bei der die stochastische Verteilung der Szenarien bzw. Umweltzustände ex ante bekannt ist. Um das Risikoverständnis im Hinblick auf die finanzielle Auswirkung zu vervollständigen, ist die wirkungsbezogene Sichtweise zu integrieren. Risiko ist hiernach die Abweichung (*Effect*) von einem definierten Sollzustand. Dies kann negativ, in Form eines finanziellen Verlusts (*Loss*), oder positiv, als zusätzlicher Gewinn (*Gain*), interpretiert werden.

$$Loss \sqcup Gain \sqsubseteq Effect \tag{3.3}$$

Dem Risikoverständnis aus Definition 2.1 folgend werden nur finanzielle Verluste als Risiko betrachtet. Die Verbindung zwischen der extensiven Risikofassung und dem wirkungsbezogenen Begriff entsteht dadurch, dass Verluste nicht losgelöst von der Wertkette entstehen, sondern direkt durch die einzelnen Ak-

tivitäten verursacht (*generate*) werden. Das allgemeine Geschäftsrisiko wird ausschließlich als finanzieller Verlust im Umfeld der Aktivitäten einer Wertkette verstanden, der aufgrund von Einflussgrößen, deren Zustände bekannten Wahrscheinlichkeitsverteilungen folgen (*determine*), eintritt.

$$BusinessRisk \equiv Loss \sqcap \exists\ determine.\{probability\} \qquad (3.4)$$

Abbildung 3.2 stellt die Ontologie allgemeiner Geschäftsrisiken dar. Die gewählte graphische Notation ist an die Description Logic angelehnt. Die Ontologie verkörpert einen Querschnitt aus den unterschiedlichen, existierenden Risikobegriffen. Das Hauptaugenmerk dieser Arbeit liegt auf der Entwicklung eines grundlegenden Verständnisses operationeller Risiken.

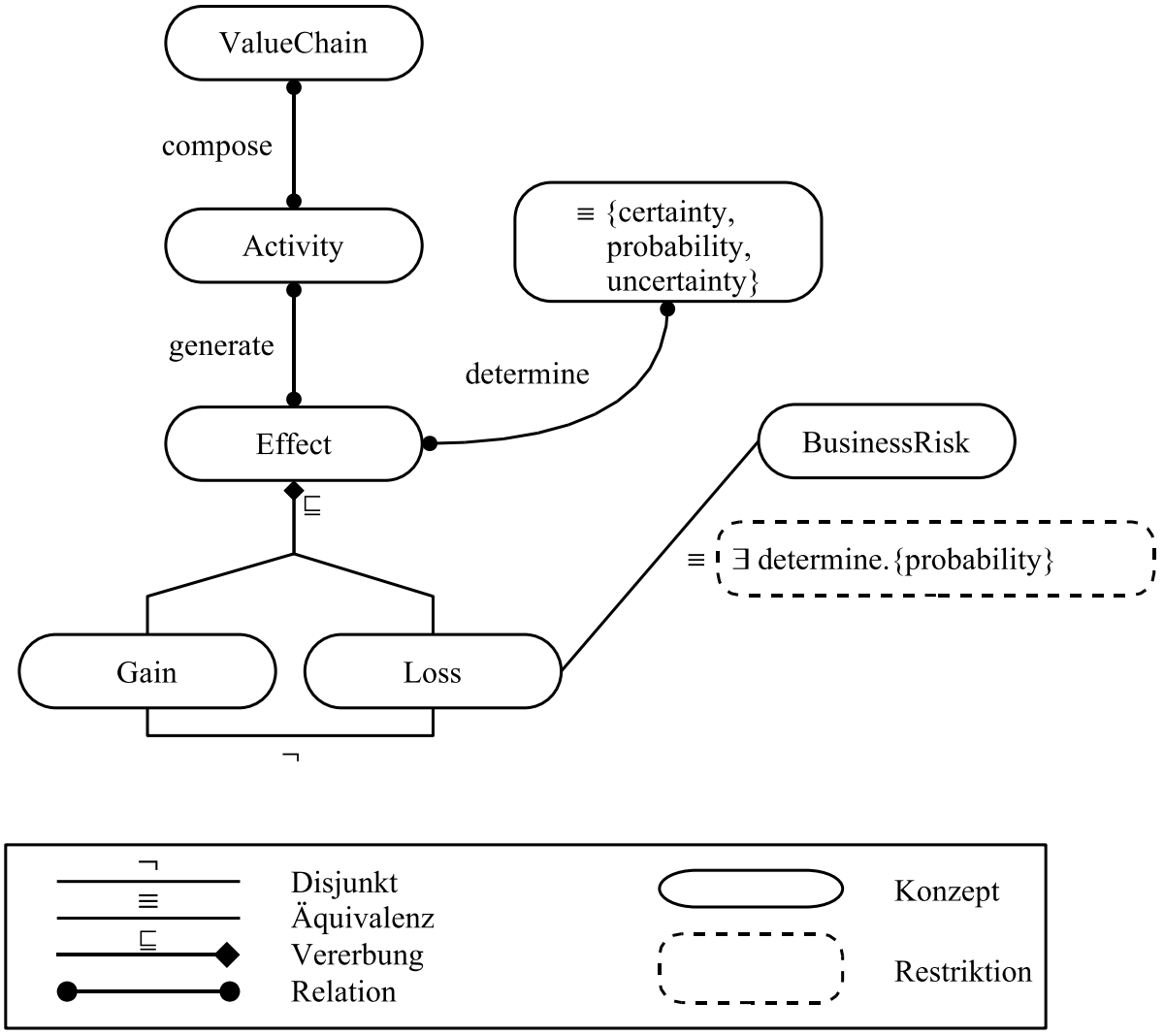

Abbildung 3.2: Ontologie allgemeiner Geschäftsrisiken

3.2.2 Operationelle Risiken bei Kreditinstituten

Eine weitere wichtige Grundlage für Technologierisiken sind die operationellen Risiken nach Basel II. Im Bankenumfeld stellen diese den wesentlichen Rahmen für die aufsichtsrechtliche Berücksichtigung technologischer Risiken dar. Daher sollten Technologierisiken bei Banken stets auch als Teil der operationellen Risiken betrachtet werden. Ausgangspunkt der folgenden Begriffsentwicklung ist die in Kapitel 2.1.2 hergeleitete Definition 2.2 operationeller Risiken.

Um eine klare Differenzierung von den klassischen Risiken des Bankgeschäfts vorzunehmen, wird in Residualdefinitionen eine Abgrenzung zu den Begriffen Marktrisiko (*MarketRisk*), Kreditrisiko (*CreditRisk*) sowie Zinsänderungsrisiko (*InterestRateRisk*) vorgenommen.

$$\begin{aligned} &\mathit{OperationalRisk} \sqsubseteq \neg\ \mathit{MarketRisk} \\ &\mathit{OperationalRisk} \sqsubseteq \neg\ \mathit{CreditRisk} \\ &\mathit{OperationalRisk} \sqsubseteq \neg\ \mathit{InterestRateRisk} \end{aligned} \tag{3.5}$$

Da ein solcher Ansatz keinen eigentlichen Beitrag zum Verständnis liefert, wird nachfolgend der Kernaspekt operationeller Risiken hervorgehoben. Hiernach resultieren operationelle Risiken ausschließlich aus dem Betrieb der Wertkette eines Unternehmens. Dabei verursachen die Ressourcen (*Resource*), die für das Betreiben (*operate*) der Aktivitäten zwingend erforderlich sind, Störungen im Ablauf der Wertschöpfung.

$$\mathit{Resource} \equiv \exists\ \mathit{operate}\,.\,\mathit{Activity} \tag{3.6}$$

Die Beziehung zwischen den Aktivitäten und Verlusten gestaltet sich dann entsprechend dem Konzept der allgemeinen Geschäftsrisiken (vgl. Abbildung 3.2). Die Ursachen für die auftretenden Betriebsstörungen liegen in zugeordneten (*exhibit*) Eigenschaften (*Property*), deren Zustände die Funktionstüchtigkeit der Ressource verkörpern.

Da die aufsichtsrechtliche Betrachtung entsprechend Basel II im Rahmen dieser Arbeit eine hervorgehobene Stellung einnimmt, wird das dort entwickelte Verständnis operationeller Risiken genutzt, um die Definition zu verfeinern. Operationelle Risiken werden hier als mögliche Verluste aus Prozessschwächen, menschlichem Versagen oder Störungen im technologischen Umfeld definiert. Darüber hinaus werden in Basel II mögliche Verluste aus externen Ereignissen betrachtet. Weil hier die Wertkette und ihr Betrieb im Mittelpunkt der ursachenbezogenen Betrachtung steht, werden externe Risiken (*ExternalEvent*) nicht direkt berücksichtigt.

Die internen, operationellen Risiken aus Prozessen (*Process*), Menschen (*Human*) und Technologie (*Technology*) werden auf die Ressourcen abgebildet und der eingeführte Begriff so konkretisiert.

$$Process \sqcup Human \sqcup Technology \sqsubseteq Resource \tag{3.7}$$

Rechtliche Risiken, wie Geldstrafen, sind in diesem Verständnis entsprechend Basel II implizit enthalten. Nicht Bestandteil der Betrachtung sind jedoch Strategierisiken (*StrategyRisk*) oder Reputationsrisiken (*ReputationRisk*).

$$\begin{aligned} OperationalRisk &\sqsubseteq \neg\ StrategyRisk \\ OperationalRisk &\sqsubseteq \neg\ ReputationRisk \end{aligned} \tag{3.8}$$

Um die Modellierung auf die von Basel II geforderte Systematik aus Geschäftsfeld (*BusinessLine*) und Ereignistyp (*EventType*) abbilden zu können, werden die Aktivitäten und Eigenschaften den Basler Kategorien zugeordnet (*map*). Dabei entsprechen die Konzepte der Geschäftsfelder und Ereignistypen den in den Anhängen 8 und 9 der Basler Richtlinie genannten Einteilungen. Formel 3.9 enthält die Formalisierung von *BusinessLine*, *EventType* erfolgt analog.

$$\begin{aligned} BusinessLine \equiv \{ &corporateFinance, tradingSales, \\ &retailBanking, commercialBanking, \\ &paymentSettlement, agencyServices, \\ &assetManagement, retailBrokerage\} \end{aligned} \tag{3.9}$$

Die möglichen Verluste werden weiter untergliedert (siehe Cap Gemini Ernst & Young 2002). Im einfachsten Fall führen die Risiken zu direkten Auszahlungen (*Payment*). Ferner sind bilanzielle Effekte, wie Abschreibungen oder Zuführungen zu Rückstellungen möglich, die zu Aufwänden (*Expense*) führen. Auch stellen entgangene Gewinne (*MissedGain*) eine weitere Verlustart dar.

$$Payment \sqcup Expense \sqcup MissedGain \sqsubseteq Loss \tag{3.10}$$

Operationelle Risiken werden auf Basis allgemeiner Geschäftsrisiken (vgl. Formel 3.4) definiert, wobei die Verluste dadurch verursacht werden, dass eine Ressource die ausreichende Unterstützung des Betriebs der Wertkette nicht mehr gewährleistet.

$$\begin{aligned} OperationalRisk \equiv\ &Loss \sqcap \exists\ determine.\{probability\} \\ &\sqcap \exists\ operate.Resource \end{aligned} \tag{3.11}$$

Die vorgestellten Konzepte zu operationellen Risiken werden in Abbildung 3.3 zusammengefasst.

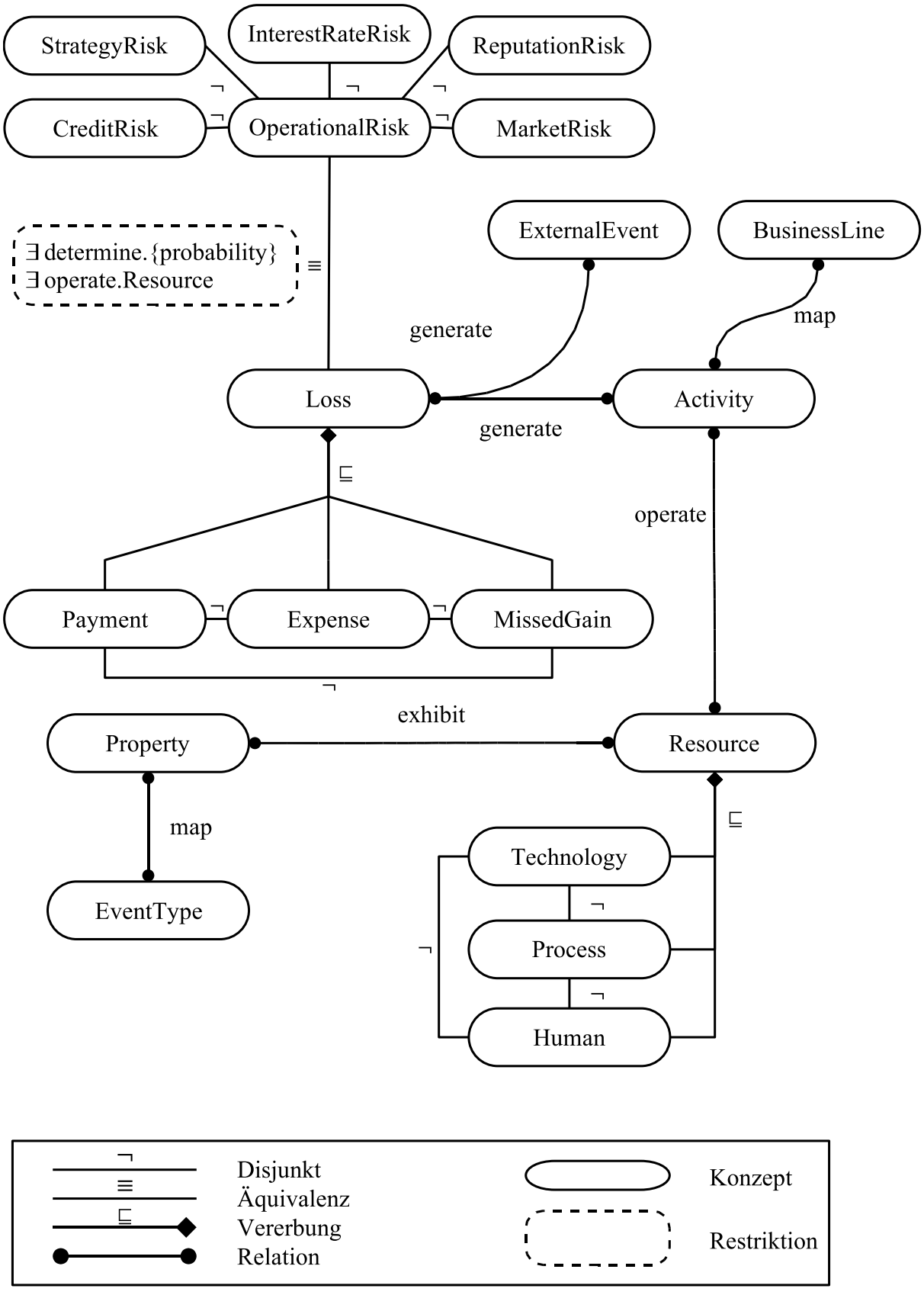

Abbildung 3.3: Ontologie operationeller Risiken

3.2.3 Technologie-Ressourcen und Eigenschaften

Ziel der zu entwickelnden Ontologie ist die Formalisierung eines Modells technologischer Risiken, das Aspekte des Basler Verständnisses und der IT-Governance auf Basis der dargestellten Ansätzen allgemeiner und operationeller Risiken verbindet. Grundgedanke dabei ist, dass Technologierisiken durch Ressourcen aus dem technologischen Umfeld der Bank verursacht werden. Das Konzept *Technology* wird hierzu aufgegriffen und mit den Ergebnissen aus der Phase der Spezifikation (vgl. Tabelle 3.1) konkretisiert. Damit werden die technologischen Ressourcen gemäß den Ebenen in atomare IT-Komponenten (*ITComponent*), komplexe Anwendungssysteme (*ApplicationSystem*) und funktionale Aufgaben des IT-Managements (*ITManagementTask*) unterteilt.

$$ITComponent \sqcup ApplicationSystem \sqcup ITManagementTask \sqsubseteq Technology \tag{3.12}$$

Die IT-Komponenten umfassen im Wesentlichen Geräte mit materieller Eigenschaft (*Hardware*), ausführbare Programme (*Software*), technische Verbindungen von IT-Komponenten (*Network*) oder die erforderliche physische Infrastruktur (*Infrastructure*) (vgl. Probst 2003, S.22ff.).

$$Hardware \sqcup Software \sqcup Infrastructure \sqcup Network \sqsubseteq ITComponent \tag{3.13}$$

Das Anwendungssystem wird technisch als die Zusammensetzung (*form*) von verschiedenen IT-Komponenten (vgl. Tabbert 2003, S.32ff.; Stahlknecht und Hasenkamp 1997, S.242ff.) interpretiert. Eine zusätzliche Sichtweise ist die fachliche Funktion, die ein Anwendungssystem im Rahmen der Leistungserstellung übernimmt. Die informationstechnische Komponente der Wertkette (vgl. Volck 1997, S.38) wird somit durch die Anwendungssysteme ermöglicht. Die Komplexität der Informationsflüsse innerhalb der Bank wird über die Relation *depend* ausgedrückt, die beschreibt, dass ein Anwendungssystem jeweils von einem anderen direkt abhängt.

$$\geqslant 1\ depend \sqsubseteq ApplicationSystem$$
$$\top \sqsubseteq \forall\ depend\,.\,ApplicationSystem \tag{3.14}$$

Neben den grundlegenden IT-Komponenten und Anwendungssystemen haben die notwendigen Veränderungen in den Phasen des Systemlebenszyklus Einfluss auf Technologierisiken (vgl. Gaulke 2002, S.7). Diese IT-Managementaufgaben können entweder als einmalige Vorhaben im Rahmen eines internen Projekts (siehe Versteegen 2003) oder im regelmäßigen IT-Betrieb erfolgen. Wird der Systemlebenszyklus als Strukturierungshilfe verwendet, können diese Auf-

gaben in die Entwicklung (*Development*), die Einführung (*Introduction*), den Betrieb (*Operation*), die Umstellung (*Migration*) oder die Ablösung (*Termination*) von Anwendungssystemen unterteilt werden (vgl. Peuker 1994, S.31).

$$Development \sqcup Introduction \sqcup Operation \sqcup Migration \sqcup Termination \sqsubseteq ITManagementTask \quad (3.15)$$

Zur Laufzeit können IT-Managementaufgaben die Ordnungsmäßigkeit der betroffenen Anwendungssysteme beeinflussen (*influence*). Die Einteilung der technologischen Ressourcen in drei Ebenen sowie deren Konkretisierung ist in Abbildung 3.4 zusammengefasst.

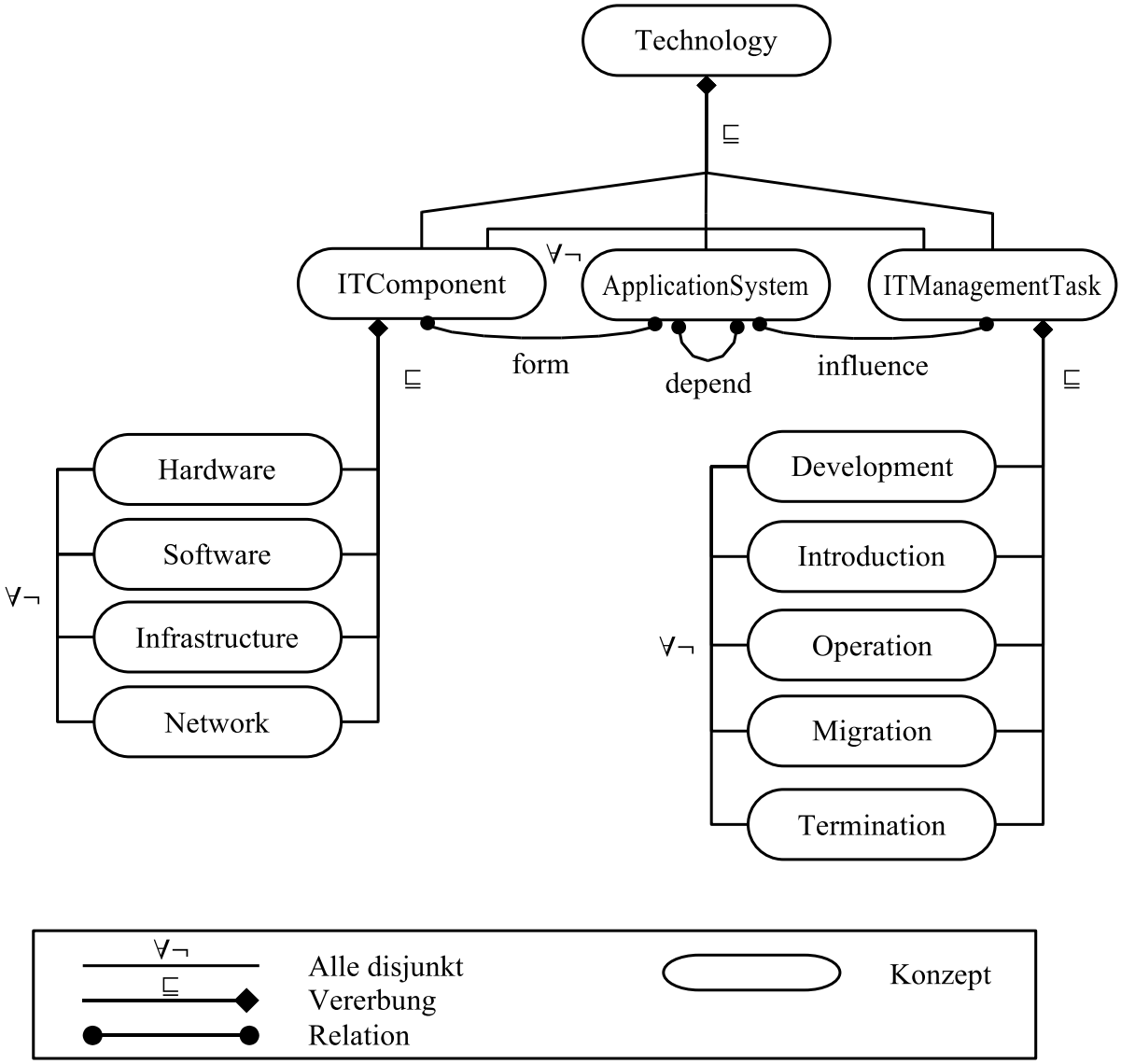

Abbildung 3.4: Technologierisiko-Ontologie (Ebenen)

Als wichtiger Aspekt einer ursachenbezogenen Risikobetrachtung sind die beeinflussenden Eigenschaften (*Property*) der Ressourcen einzubeziehen. Entsprechend der Übersicht aus Tabelle 3.2 werden die Eigenschaften der IT-Komponenten unter Sicherheit (*Security*), die der Anwendungssysteme unter Ordnungsmäßigkeit (*Compliance*) und die der IT-Managementaufgaben unter Zuverlässigkeit (*Soundness*) zusammengefasst. Im Folgenden werden die jeweils wichtigsten Eigenschaften erläutert. Diese Taxonomie ist nicht abgeschlossen, so dass anwendungsspezifische Erweiterungen möglich sind.

$$\mathit{Security} \sqcup \mathit{Compliance} \sqcup \mathit{Soundness} \sqsubseteq \mathit{Property} \tag{3.16}$$

Für die IT-Komponenten wird Risiko mit nicht vorhandener Sicherheit gleichgesetzt (vgl. Hammer 1999, S.98). IT-Komponenten beeinträchtigen Anwendungssysteme, wenn beispielsweise die Eigenschaft der Funktionstüchtigkeit (*Integrity*), der Verfügbarkeit (*Availability*) oder der Vertraulichkeit (*Confidentiality*) nicht gegeben ist.

$$\mathit{Integrity} \sqcup \mathit{Availability} \sqcup \mathit{Confidentiality} \sqsubseteq \mathit{Security} \tag{3.17}$$

Der ordnungsmäßige Betrieb der Wertkette erfordert es mindestens, dass die Richtigkeit (*Correctness*), Vollständigkeit (*Completeness*) und die Zeitgerechtheit (*Timeliness*) der Systeme gewährleistet ist. Weitere, im Prüfungsstandard IDW RS FAIT 1 festgelegte Eigenschaften, sind durch die gewählte Formalisierung nicht explizit ausgeschlossen.

$$\mathit{Correctness} \sqcup \mathit{Completeness} \sqcup \mathit{Timeliness} \sqsubseteq \mathit{Compliance} \tag{3.18}$$

Abschließend beeinflussen Vorhaben im Rahmen des Systemlebenszyklus die Ordnungsmäßigkeit der Anwendungssysteme genau dann, wenn die Ziele Effektivität (*Effectiveness*), Effizienz (*Efficiency*) und insbesondere bei IT-Projekten (vgl. Gaulke 2002, S.13f.) Termingerechtheit (*Schedule*) gefährdet sind.

$$\mathit{Effectiveness} \sqcup \mathit{Efficiency} \sqcup \mathit{Schedule} \sqsubseteq \mathit{Soundness} \tag{3.19}$$

Um die Zuordnung der Eigenschaften auf die jeweiligen Ressourcen einzuschränken, müssen zusätzlich Restriktionen definiert werden.

$$\begin{aligned} &\mathit{ITManagementTask} \sqsubseteq \forall\, \mathit{exhibit}\,.\,\mathit{Soundness} \\ &\mathit{ApplicationSystem} \sqsubseteq \forall\, \mathit{exhibit}\,.\,\mathit{Compliance} \\ &\mathit{ITComponent} \sqsubseteq \forall\, \mathit{exhibit}\,.\,\mathit{Security} \end{aligned} \tag{3.20}$$

Die folgende Abbildung 3.5 zeigt die im Rahmen dieser Arbeit verwendete Taxonomie der Eigenschaften.

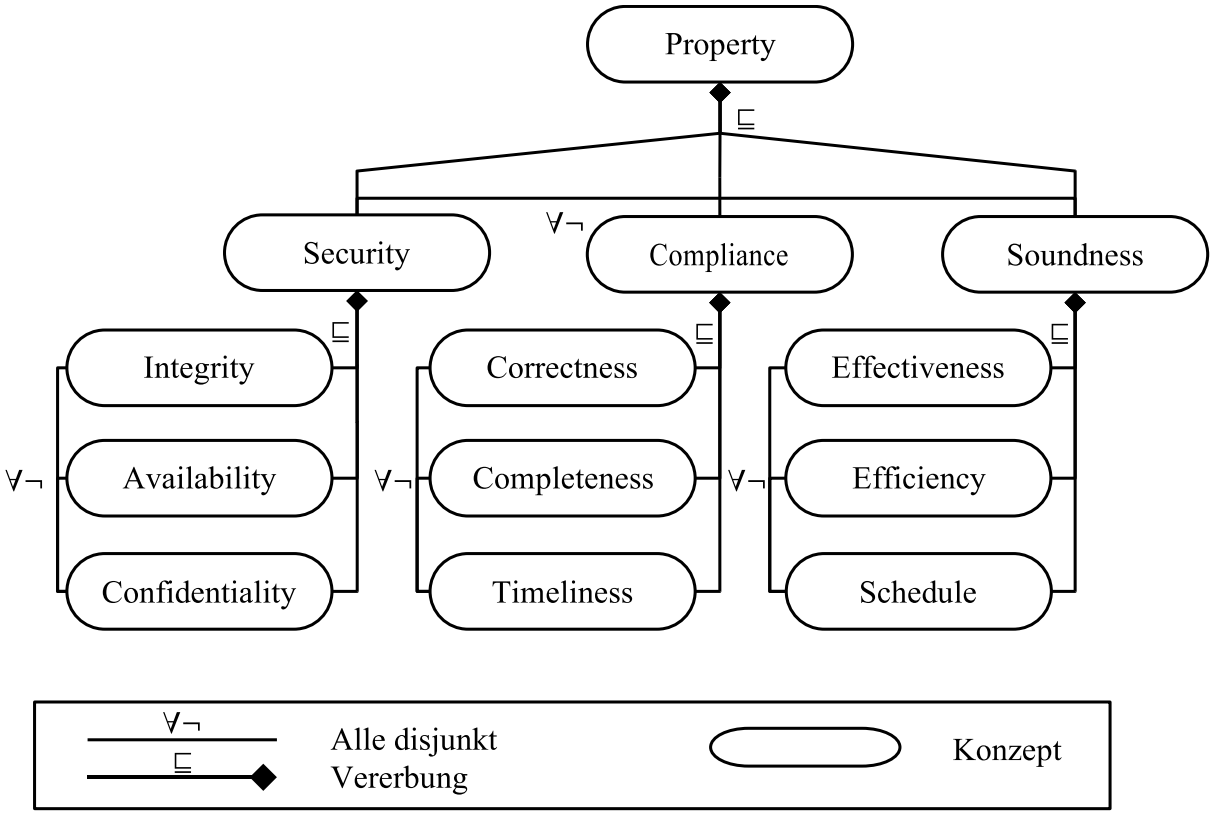

Abbildung 3.5: Technologierisiko-Ontologie (Eigenschaften)

3.2.4 Zusammenfassende Darstellung

Die verschiedenen Aspekte der Ontologie aus den vorangegangenen Kapiteln werden zu einem Verständnis der Technologierisiken vereinigt und auf die zentralen Konzepte verengt. Als Technologierisiken werden im Rahmen dieser Arbeit Verluste bezeichnet, die mit einer bekannten Wahrscheinlichkeit eintreten und aus dem Versagen einer technologischen Ressource resultieren.

$$\begin{aligned} \mathit{TechnologyRisk} \equiv\ & \mathit{Loss} \sqcap \exists\ \mathit{determine}.\{\mathit{probability}\} \\ & \sqcap \exists\ \mathit{operate}.\mathit{Technology} \end{aligned} \tag{3.21}$$

Die für die Technologierisiko-Ontologie zentralen Konzepte und Relationen sind in der folgenden Abbildung 3.6 visualisiert. Entscheidend ist, dass diese Formalisierung nicht als abgeschlossen angesehen werden muss. Die Konzepte können nach Bedarf weiter verfeinert oder erweitert werden. So kann die Ontologie an die individuellen Anforderungen einer Bank angepasst werden, ohne auf die vorgegebene Struktur zu verzichten. Des Weiteren sind Umbenennungen oder Einschränkungen auf Basis der festgelegten Kernbestandteile möglich.

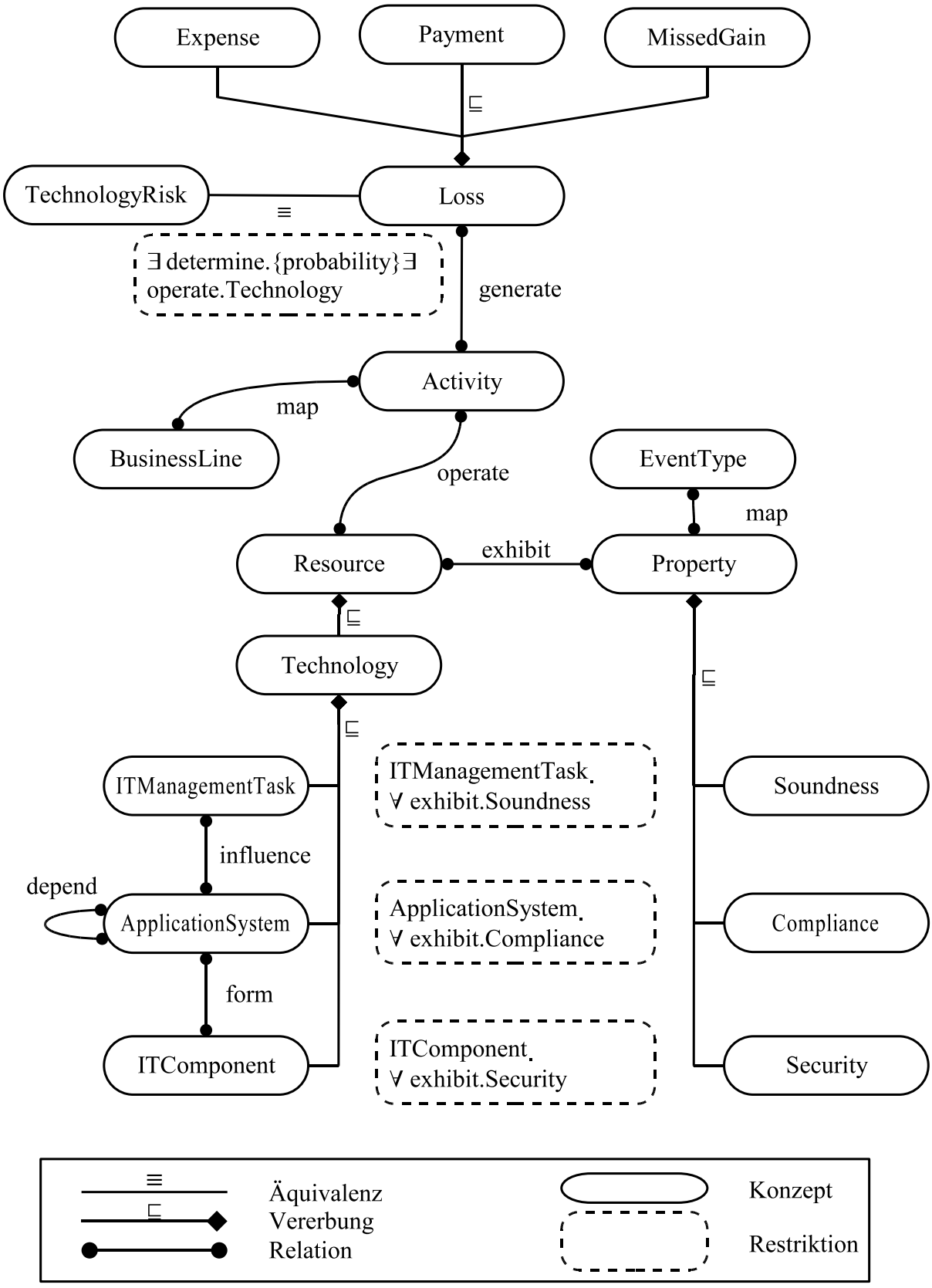

Abbildung 3.6: Technologierisiko-Ontologie (Gesamt)

3.3 Evaluation

Aufgrund der hervorgehobenen Bedeutung der Technologierisiko-Ontologie für die in dieser Arbeit entwickelte Methode zur Risikoquantifizierung ist eine Überprüfung der Konzepte und Relationen unabdingbar. Um die Einsatzfähigkeit der Ontologie zu überprüfen, werden die in Kapitel 2.3.2 vorgestellten Methoden zur Evaluation eingesetzt. Die dargestellte Taxonomie wird zum einen mittels der OntoClean-Methode auf eine konsistente Vererbungshierarchie hin untersucht, zum anderen wird der fachlichen Sicht der Anwendbarkeit über die Bewertung der Dimensionen Abdeckung und Präzision Rechnung getragen.

Nach der OntoClean-Methode werden den kritischen Konzepten der Technologierisiko-Ontologie Ausprägungen für vier Meta-Eigenschaften zugewiesen und daraus die Konzeptgruppen abgeleitet (vgl. Kapitel 2.3.2). Tabelle 3.3 (Reihenfolge entsprechend der Taxonomie) zeigt das Ergebnis dieser Klassifizierung für die zentralen Konzepte der Ontologie:

Konzept	**Meta-Eigenschaften**				**Konzept-gruppe**
	Identität	Rigidität	Abhängigkeit	Einheit	
TechnologyRisk	+O / +I	+R	+D	-U	Typ
Loss	-O / -I	+R	+D	-U	Kategorie
Expense	-O / +I	-R	+D	-U	Rolle
Payment	-O / +I	-R	+D	-U	Rolle
MissedGain	-O / +I	-R	+D	-U	Rolle
Activity	+O / +I	+R	-D	+U	Typ
BusinessLine	-O / -I	-R	-D	-U	Attribut
EventType	-O / -I	-R	-D	-U	Attribut
Resource	-O / -I	+R	-D	+U	Kategorie
Technology	-O / -I	+R	-D	+U	Kategorie
ITManagementTask	-O / -I	+R	-D	+U	Kategorie
ApplicationSystem	-O / -I	+R	-D	+U	Kategorie
ITComponent	-O / -I	+R	-D	+U	Kategorie
Property	-O / -I	+R	-D	-U	Kategorie
Soundness	-O / -I	+R	-D	-U	Kategorie
Compliance	-O / -I	+R	-D	-U	Kategorie
Security	-O / -I	+R	-D	-U	Kategorie

Tabelle 3.3: Zuweisung Meta-Eigenschaften nach OntoClean

Eine Auswertung der Einschränkungen und Annahmen nach der OntoClean-Methode (vgl. Formel 2.10) ergibt keine Widersprüche für die der Ontologie zugrunde liegende Basis-Taxonomie.

Eine formale Beweisführung der inhaltlichen Korrektheit ist jedoch nicht möglich. *„[...] we cannot prove the completeness of an ontology nor the completeness of its definitions [...]“* (Gomez-Perez, Fernandez-Lopez und Corcho 2004, S.179). Allgemein formuliert können Ontologien jeweils nur eine approximative Konzeptualisierung einer Spezifikation verkörpern (vgl. Guarino und Persidis 2003, S.4). Jedoch kann und muss der Grad der jeweiligen Annäherung analysiert werden. Für die folgende Diskussion der Dimensionen Abdeckung und Präzision wird das beabsichtigte Modell I_K im Hinblick auf die Konzeptualisierung K zugrunde gelegt, das über das Motivating Scenario sowie die Competency Questions (vgl. Kapitel 3.1.5, Fragen Q1 - Q3.3) spezifiziert ist.

Entscheidend für beide Begriffe (vgl. Formeln 2.11 und 2.12) ist die Schnittmenge aus dem ontologischen Modell der Technologierisiken O_K und I_K. Zur Analyse der Schnittmenge müssen die relevanten Fragen (vgl. Kapitel 3.1.5) mit der Ontologie abgeglichen werden: Ein Verständnis allgemeiner Geschäftsrisiken (Q1) ist in der Ontologie als Konzept *BusinessRisk* enthalten. Der Anforderung nach der Einschränkung auf operationelle Risiken gemäß Basel II (Q2.1) sowie der Verbindung mit der Wertkette der Bank (Q2.2) wird durch die Konzeptualisierung von *OperationalRisk* in Verbindung mit *ValueChain* entsprochen. Die Begriffsbildung der Technologierisiken erfolgt unter Berücksichtigung von Standards wie COBIT oder IDW PS 330, so dass den Aspekten der IT-Governance (Q3.1) Rechnung getragen wird. Die Hierarchien von *Technology* und *Property* entsprechen den Fragen Q3.2 und Q3.3.

Für die Abdeckung ist das Verhältnis zwischen der Schnittmenge $O_K \cap I_K$ und dem Umfang von I_K relevant. Das impliziert die Frage, ob O_K konkrete, von der Spezifikation vorgesehene Aspekte nicht ausreichend berücksichtigt. Dabei soll nicht generell untersucht werden, ob die Ontologie sämtliche Aspekte des Risikomanagements oder der IT-Governance umsetzt. Stattdessen muss ausschließlich auf Ebene der Competency Questions eine vollumfängliche Abdeckung durch O_K gewährleistet sein. Damit ist dann indirekt auch $I_K \subseteq O_K$ gegeben.

Die Untersuchung der Präzision wendet sich der Frage zu, ob sich aus der Ontologie nicht beabsichtigte Aussagen ableiten lassen. Das Verhältnis $O_K \cap I_K$ zu O_K lässt sich nur vergleichsweise eingeschränkt abschätzen. Da sich hieraus für die Zielsetzung dieser Arbeit erst einmal keine Limitationen ergeben, wird dieser Aspekt hier nicht weiter verfolgt.

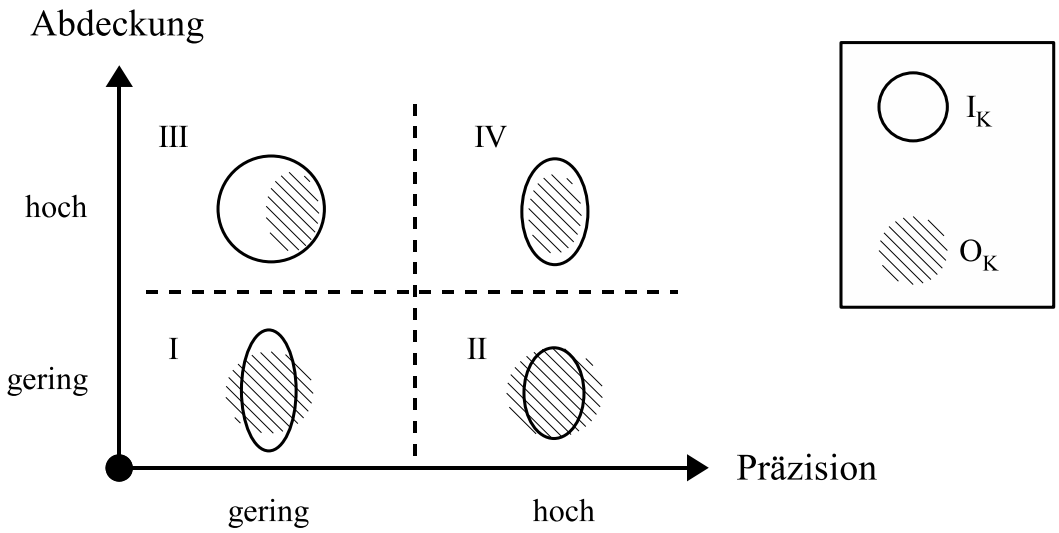

Abbildung 3.7: Gegenüberstellung Präzision und Abdeckung
(siehe Guarino und Persidis 2003)

Um die Güte einer Ontologie zu beurteilen, unterscheiden Guarino und Persidis vier Kombinationen (vgl. Abbildung 3.7) der Kriterien Präzision und Abdeckung (vgl. Guarino und Persidis 2003, S.6). Im Sinne der bisherigen Argumentation wird eine hinreichende Abdeckung unterstellt.

Da die Präzision deutlich schwieriger zu beurteilen ist, wird dieses Kriterium lediglich indirekt in die Beurteilung miteinbezogen. Unabhängig davon kann jedoch aufgrund der Formalisierung über eine axiomatische Theorie von einem adäquaten Präzisionsgrad ausgegangen werden (vgl. Guarino und Persidis 2003, S.8). Die im Rahmen dieser Arbeit entwickelte Technologierisiko-Ontologie kann also mindestens zwischen den Quadranten III und IV eingeordnet werden.

3.4 Zusammenfassung

Als erstes Ziel wird in Kapitel 1 das Verständnis der Technologierisiken genannt. Zentraler Bestandteil hiervon sind die Entzerrung der begrifflichen Unstimmigkeiten sowie die Verbindung der Sichtweise nach Basel II mit akzeptierten Ansätzen aus der IT-Governance (vgl. Kapitel 1.2, Ziel 1a). Dieses wird in dieser Arbeit über die Entwicklung einer formalen Ontologie für Technologierisiken umgesetzt.

Zur Untermauerung der These werden die wesentlichen Vorteile formaler Ontologien herangezogen:

„[...] ontologies reduce conceptual and terminological confusion by providing a unifying framework within an organisation. In this way, ontologies enable shared understanding and communication between people with different needs and viewpoints arising from their particular contexts.“ (Uschold und Grüninger 1996, S.8)

Durch die Schaffung eines normativen Modells auf Basis formaler Ontologien kann ein gemeinsames Verständnis technologischer Risiken erreicht werden, welches das enthaltene Wissen explizit formuliert (vgl. Uschold und Grüninger 1996, S.8). Die Vorteilhaftigkeit formaler Ontologien für die Modellierung von Technologierisiken spiegelt sich auch in den Basler Anforderungen wider:

“Whatever the exact definition, a clear understanding by banks of what is meant by operational risk is critical to the effective management and control of this risk category.” (BCBS 2003b, Tz.5)

Genauso wichtig wie ein gemeinsames Verständnis ist die Entwicklung eines nach Möglichkeit widerspruchsfreien Modells, das präzise Begriffe prägt (vgl. Uschold und Grüninger 1996, S.9). Diesem Aspekt kommt insbesondere bei der automatischen Verarbeitung durch Software eine besondere Bedeutung zu. Der Zustand der Widerspruchsfreiheit muss ferner auch bei einer Weiterentwicklung des Modells technologischer Risiken aufrechterhalten werden. In diesem Zusammenhang ist auch die Möglichkeit hervorzuheben, Synonyme innerhalb der Ontologie zu definieren, ohne die Konsistenz zu beeinträchtigen.

Nicht nur Begriffe sondern auch Relationen können über Ontologien modelliert werden (vgl. Uschold und Grüninger 1996, S.8). Dies kann zum einen dazu genutzt werden, die Beziehungen zwischen den Konzepten der Technologierisiko-Ontologie formal darzustellen, zum anderen können die Zusammenhänge verschiedener Elemente innerhalb der Wertschöpfung einer Bank explizit abgebildet werden (vgl. Kapitel 1.2, Ziel 1b).

Im Sinne der Zielsetzung dieser Arbeit ist schließlich noch ein weiterer Aspekt relevant (vgl. Kapitel 1.2, Ziel 1c). Durch die Verwendung formaler Ontologien zur Repräsentation der Konzepte und Strukturen im Umfeld der Technologierisiken, ist es möglich, individuelle Erweiterungen oder Einschränkungen am Modell vorzunehmen. Solche Veränderungen können über einen Wissensmanagementprozess gesteuert werden. Ferner können geplante Änderungen innerhalb der Informationstechnologie ex ante im Modell erfasst und Szenarien so durchgespielt werden.

Abschließend soll ein übergreifender Aspekt beleuchtet werden, der die Überleitung zu den folgenden Kapiteln ermöglicht. Ontologien können auch verwendet werden, um verschiedene Sichtweisen auf ein zentrales Modell zu ermöglichen (vgl. Uschold und Grüninger 1996, S.9ff.). Hiermit ist nicht nur die Verbindung unterschiedlicher Interpretationen des Risikobegriffs zur Entwicklungszeit der Ontologie gemeint, sondern auch der Aspekt der technischen Kommunikation. Durch jeweils spezifische Sichten können unterschiedliche Methoden innerhalb des Risikomanagementprozesses Teile des Modells extrahieren und mit eigenen Informationen anreichern.

Im folgenden Kapitel wird die Ontologie-zentrierte Quantifizierung operationeller Technologierisiken beschrieben, die eine solche spezifische Sicht auf das Modell darstellt. Die Implementierung der Ontologie-zentrierten Methode ist Bestandteil von Kapitel 5. Hierbei steht dann die Entwicklung der Ontologie in OWL sowie die Umsetzung der Sichten im Vordergrund.

Kapitel 4
Methode zur Quantifizierung

In diesem Kapitel steht die Schaffung einer Methode zur Umsetzung des zweiten zentralen Ziels dieser Arbeit – Quantifizierung der Technologierisiken – im Vordergrund. Das Hauptaugenmerk liegt dabei auf einer möglichst unvoreingenommenen und zielgerichteten Ermittlung des finanziellen Risikopotentials aus Technologierisiken. Dabei stellt die Integration des zugrunde liegenden Verständnisses beziehungsweise Wissens aufgrund der vorherrschenden Unklarheiten auch für quantitative Methoden eine wichtige Grundlage dar:

„[...] risk management is about managing the complexity inherent in the trade off between return and risk, through organizational knowledge, for the benefit of the firm's stakeholders.“ (Marshall, Prusak und Shpilberg 1996, S.81)

Der Begriff Wissen bezeichnet entsprechend der Auffassung dieser Arbeit das gesamte Verständnis, das Individuen dazu befähigt, ein bestimmtes Problem zu lösen (vgl. Kapitel 2.3.1), hier die Quantifizierung operationeller Technologierisiken. Entscheidend für die Darstellung solchen Wissens ist eine gemeinsame Sprache (siehe Davenport und Prusak 1998), die die verwendeten Begriffe und ihre Bedeutung einheitlich festlegt. In Bezug auf operationelle Technologierisiken kommen weiterhin dem organisatorischen Wissen über technologische Strukturen sowie der Reflektion möglicher Veränderungen durch einen Wissensmanagementprozess eine besondere Bedeutung zu.

In den folgenden Abschnitten wird zunächst ein allgemeiner Überblick der Ansätze zur Quantifizierung operationeller Risiken gegeben. Es werden die jeweiligen zugrunde liegenden Modelle identifiziert und die zugehörigen Methoden dargestellt. Diese werden im Hinblick auf zwei Ziele untersucht: Die Integration des Verständnisses dieser Risikokategorie und die Eignung hinsichtlich der Quantifizierung operationeller Technologierisiken. Aufgrund der identifizierten Schwächen, insbesondere im Hinblick auf das erste Ziel, wird als neuer Ansatz eine Ontologie-zentrierte Simulation auf Basis des in Kapitel 3.2 vorgestellten Modells operationeller Technologierisiken vorgeschlagen und kritisch bewertet.

4.1 Quantifizierung im Risikomanagement

Zur Unterstützung eines ganzheitlichen Risikomanagements in Kreditinstituten wurde eine große Anzahl an Methoden für den Bereich operationeller Risiken entwickelt. In der Literatur werden diese in der Regel anhand des Einsatzes in den verschiedenen Phasen des Risikomanagementprozesses dargestellt und untersucht (siehe Horn und Müller 2001; Füser, Rödel und Kang 2002; Piaz 2002; Faisst 2004; Minz 2004).

Darüberhinaus werden auch isoliert die Methoden aus der Phase der Quantifizierung beschrieben und verglichen (siehe King 2001; Cruz 2002; Smithson und Song 2004). In den folgenden Absätzen wird ein Überblick der wesentlichen Methoden zur Quantifizierung gegeben und diese im Spannungsfeld zwischen der bankeigenen und der aufsichtsrechtlichen Sichtweise dargestellt. Aus der Vielzahl der in der Literatur vorgestellten Methoden zur Quantifizierung operationeller Risiken können anhand der zugrunde liegenden Modelle drei Ansätze zusammengefasst werden (vgl. Smithson und Song 2004, S.57f.):

- Einfache Methoden modellieren das Risiko direkt über beeinflussende Größen. Hierunter fällt auch der von Basel II vorgeschlagene Basisindikator- beziehungsweise Standardansatz, der das Risikopotential über den Bruttoertrag abschätzt.
- Fortgeschrittene Methoden (AMA) basieren im Kern auf dem versicherungstechnischen Modell. Hier werden zukünftige Verluste über die Wahrscheinlichkeitsverteilungen von Häufigkeit und Verlusthöhe messbar gemacht. Gängige Methoden zur Schätzung des Risikopotentials sind hier das Self-Assessment, die Speicherung historischer Verluste in einer Verlustdatenbank, die Extremwerttheorie oder Indikatoransätze.
- Auf einem Modell kausaler Zusammenhänge und funktionaler Abhängigkeiten basierende Methoden reflektieren unmittelbar die Risikosituation in der Bank, um daraus das operationelle Risikopotential abzuleiten.

Die obige Klassifizierung der Modelle sowie der darin verwendeten Methoden ist stark an Basel II angelehnt, da die aktuelle Diskussion noch wesentlich durch die regulatorische Betrachtung getrieben wird. Insbesondere die Methoden zur Ermittlung einer Verlustverteilung stehen in einer engen Beziehung zu den Anforderungen an das Management operationeller Risiken nach AMA (vgl. Basel II, Tz.670ff.). Als Unterscheidungsmerkmal für die folgende Tabelle 4.1 dienen daher weniger die klassischen Kriterien, wie top-down versus bottom-up oder qualitativ versus quantitativ. Vielmehr werden die Methoden im Hinblick auf die Akzeptanz in Banken sowie die Erfüllung der regulatorischen Anforderungen untersucht.

Methode	Akzeptanz in Banken	Sichtweise Basel II
Beim **Standardansatz** (Basisindikator) werden Verluste über beeinflussende Variablen abgeschätzt.	Geringster Aufwand Über 90% der deutschen Banken planen Einsatz	Unzulässig für internationale Institute oder Banken mit hohem Risiko
Das **Self-Assessment** beschreibt die qualitative Erfassung von möglichen Eintrittswahrscheinlichkeiten und Verlusthöhen.	Wird von der Mehrheit der Banken eingesetzt Kann Fehlen empirischer Daten ausgleichen	Expertenmeinungen müssen über Szenario-Analysen erhoben werden Können quantitative Ansätze ergänzen
Eine **Verlustdatenbank** erfasst aufgetretene Schäden und ermöglicht die empirische Ermittlung von Eintrittswahrscheinlichkeiten und Verlusthöhen.	Wird als wesentliches Instrument mit Entwicklungspotential angesehen Kann zum Backtesting anderer Methoden verwendet werden	Interne Daten müssen über 5 Jahre erfasst und über externe Daten ergänzt werden Daten müssen Schema aus Geschäftsfeldern und Verlustereignissen entsprechen
Die **Extremwerttheorie** kann eingesetzt werden, um Daten im extremen Wertebereich (Tail) zu verfeinern.	Derzeit nur geringer Einsatz Analysen existierender Daten zeigen das Vorhandensein extremer Ränder	Das Risikomanagement soll extreme Verluste berücksichtigen
Der **Indikatoransatz** wird zur frühzeitigen Erkennung von Änderungen an Einflussfaktoren (Indikatoren) eingesetzt, die die Eintrittswahrscheinlichkeiten oder Verlusthöhen von Risiken verändern können.	Einsatz erfolgt im Rahmen von Frühwarnsystemen Schwierige Ermittlung kausaler Zusammenhänge zwischen Indikator und Risiko	Das Risikomanagement soll wesentliche externe und interne Indikatoren erfassen Die Beziehung zwischen Indikator und Risiko muss im Zeitverlauf validiert werden
Bei dem **Modell funktionaler Abhängigkeiten** wird die Risikoumgebung durch ein Abbild der prozessualen Abläufe und kausalen Strukturen innerhalb des Unternehmens reflektiert und daraus eine Verlustverteilung ermittelt.	Findet noch keine wesentliche Anwendung Ziel ist ein Modell der Prozesse und Strukturen Kausale Zusammenhänge sollen berücksichtigt werden	Das Modell muss Anreize zur Verbesserung des Risikomanagements geben Das Management ist für ein Verstehen der Beschaffenheit und des Umfangs der Risiken direkt verantwortlich

Tabelle 4.1: Übersicht zentraler Methoden zur Quantifizierung

Die Auswertung der Akzeptanz der einzelnen Methoden bei Kreditinstituten stützt sich auf vorliegende empirische Untersuchungen (siehe Wolf 2005; ibi research 2004), durchgeführte Studien (siehe Coleman 2000; Cap Gemini Ernst & Young 2002) sowie von der Bankenaufsicht vorgenommene Umfragen (siehe Deutsche Bundesbank und BaFin 2005). Der Abgleich mit den regulatorischen Anforderungen (siehe Basel II) basiert auf einer Gegenüberstellung der Basler Mindestanforderungen und der eingesetzten Methoden (siehe Jacobs 2004).

4.2 Synopse zentraler Ansätze

Für die dargestellten Methoden werden, gegliedert nach dem zugrunde liegenden Modell, die Umsetzung der zentralen Ziele, Verständnis und Quantifizierung operationeller Technologierisiken analysiert. Weitere Vergleichskriterien, wie mögliche Kosten bei der Einführung oder die Auswirkung der jeweiligen Methode auf das regulatorische Kapital, werden hier zunächst nicht betrachtet.

Das erste Ziel dieser Arbeit (vgl. Kapitel 1.2, Ziele 1a - 1c) wird für die Evaluation in konkrete Anforderungen an die Quantifizierungsmethode überführt (vgl. Cuske, Dickopp und Schader 2005, S.67ff.). Das durch die jeweilige Methode unterstützte Risikoverständnis wird dann anhand von drei Kriterien gemessen:

- Das Kriterium **Begriff** bezeichnet die Unterstützung eines gemeinsamen und einheitlichen Begriffsverständnisses. Entscheidend für die Beurteilung ist, ob der Methode ein solches Verständnis zugrunde liegt oder es sich zumindest integrieren lässt.
- Die Berücksichtigung des organisatorischen Wissens über das technologische Umfeld und die Zusammenhänge innerhalb des Kreditinstituts wird als **Struktur** definiert.
- Die Fähigkeit, in ein Wissensmanagement integriert, die Evolution der Begriffe und Strukturen kontinuierlich abzubilden, wird als **Dynamik** bezeichnet.

Die Unterstützung der Quantifizierung operationeller Technologierisiken durch die analysierte Methode wird anhand zweier Kriterien untersucht. Diese spiegeln das zweite zentrale Ziel der Arbeit (vgl. Kapitel 1.2, Ziele 2a + 2b) wider:

- Das Kriterium **Objektivität** liefert ein Maß für die Nachvollziehbarkeit und Unabhängigkeit der getroffenen Annahmen. In diesem Sinne ist eine Methode objektiv, wenn sie frei ist von individuellen Einschätzungen.
- Die **Risikosensitivität** beschreibt, inwiefern eine Änderung an der Risikosituation durch die ermittelten Schätzer direkt reflektiert wird.

4.2.1 Direkte Ermittlung des Risikopotentials

Eine einfache Methode zur Ermittlung des Risikopotentials ist die direkte Schätzung über beeinflussende Größen. Bei den auch als Faktor-Ansätzen bezeichneten Methoden wird entweder auf Ebene des gesamten Kreditinstitutes oder möglicherweise auf einem höheren Detaillierungsgrad das Risikopotential über Einflussfaktoren wie den Umsatz oder den Ertrag geschätzt.

„In the factor approach, the analyst attempts to identify the significant determinants of operational risk – either at the institution level or at the level of an individual business or individual process.“ (Smithson und Song 2004, S.58)

Um diese einfache Methode der Messung auch aufsichtsrechtlich zu ermöglichen, lässt Basel II eine Abschätzung der Risiken über indirekte Größen zu. Dafür werden der Basisindikator- und der Standardansatz definiert. Als Einflussfaktor für das Risikopotential wird für beide Ansätze ein durchschnittlicher Bruttoertrag der vergangenen drei Jahre herangezogen. Der Bruttoertrag des gesamten Kreditinstitutes ist dabei allgemein wie folgt definiert (vgl. Basel II, Tz.650; Rünger und Walther 2004, S.18):

	Zinsergebnis
./.	Ergebnis aus Wertpapieren
./.	Provisionsergebnis
./.	Nettoergebnis aus Finanzgeschäften
./.	sonstige ordentliche Erträge
=	**Bruttoertrag (*GI*)**

Tabelle 4.2: Ermittlung des allgemeinen Bruttoertrags

Zu beachten ist, dass *„[...] Aufwendungen, einschließlich Zahlungen an die Anbieter ausgelagerter Dienstleistungen, nicht berücksichtigt werden [...]“* (Basel II, Tz.650). Der Basisindikatoransatz definiert im einfachsten Fall das operationelle Risiko als Produkt eines festen Prozentsatzes $\alpha = 15\%$ und dem allgemeinen Bruttoertrag *GI*.

Der Standardansatz stellt eine Verfeinerung des Basisindikatoransatzes dar (vgl. Basel II, Tz.652). Bei diesem Ansatz wird das Kreditinstitut in acht Geschäftsfelder (vgl. Kapitel 2.2.1) unterteilt. Für diese wird das operationelle Risiko über die Multiplikation eines durchschnittlichen Bruttoertrags pro Geschäftsfeld

GI_i mit einem spezifischen Faktor β_i (12% bis 18%) ermittelt wird. Negative Ergebnisse in einzelnen Geschäftsfeldern dürfen sich jedoch nicht risikomindernd auswirken.

$$K_{TSA} = \frac{\sum_{Letzte\,3\,Jahre} \left(max\left(\sum_{Geschäftsfeld\,i=1}^{8} (GI_i \beta_i), 0\right)\right)}{3} \tag{4.1}$$

Die β-Faktoren für die einzelnen Geschäftsfelder wurden auf Basis von im Vorfeld der Basel-II-Einführung durchgeführten Datenerhebungen bis auf weiteres wie folgt festgelegt:

Geschäftsfeld	β-Faktor
Corporate Finance	18,00%
Trading & Sales	18,00%
Retail Banking	12,00%
Commercial Banking	15,00%
Payment & Settlement	18,00%
Agency Services	15,00%
Asset Management	12,00%
Retail Brokerage	12,00%

Tabelle 4.3: Beta-Faktoren des Standardansatzes
(vgl. Basel II, Tz.654)

Für Methoden, bei denen das Risiko über beeinflussende Größen indirekt ermittelt wird, besteht kein Zusammenhang zu einzelnen Risikokategorien. Der Standardansatz basiert demnach nicht auf einem konkreten Begriff oder expliziten Verständnis operationeller Technologierisiken. Darüberhinaus wird den strukturellen Besonderheiten des technologischen Umfelds einzelner Banken nicht Rechnung getragen. Durch die externe Festlegung der β-Faktoren wird auf Veränderungen in der Risikolandschaft nur indirekt reagiert. Die durch diese Methoden ermittelten Risikopotentiale können der Dynamik technologischer Entwicklungen deshalb nur langsam folgen.

Durch die unterschiedliche Betrachtung der acht Geschäftsfelder ist der Standardansatz differenzierter als der Basisindikatoransatz. Die Ermittlung ist aufgrund der starr vorgegebenen Struktur objektiv nachvollziehbar. Die Zuordnung des Bruttoertrags zu den Geschäftsfeldern ist hingegen nicht frei von subjekti-

ven Annahmen. Ferner ergeben sich grundsätzliche Bedenken hinsichtlich der Eignung des Bruttoertrags als Ausgangsbasis. Kritisch anzumerken ist zum Beispiel, dass die Ermittlung des Bruttoertrags abhängig von nationalen Vorschriften zur Rechnungslegung ist. Weiterhin unterliegt diese Größe gerade in Geschäftsfeldern wie Trading & Sales starken Schwankungen. Der Standardansatz ist zwar komplexer in der Implementierung als der Basisindikatoransatz, eine deutliche Erhöhung der Risikosensitivität ist jedoch nicht erkennbar (vgl. Pezier 2003, S.55). Zusammengefasst bilden diese Ansätze das Risikoumfeld zu ungenau ab, um ein effektives Risikomanagement zu ermöglichen (siehe Locher, Mehlau und Wild 2004).

4.2.2 Modellierung der Verlustverteilung

Ursachenbezogener als die indirekte Abbildung des Risikopotentials über beeinflussende Größen erscheint die Modellierung der zugrundeliegenden Verlustverteilung. Dieses sogenannte versicherungstechnische Modell hat die Abschätzung der Wahrscheinlichkeitsverteilung operationeller Verluste zum Ziel:

„An actuarial approach attempts to identify the loss distribution associated with operational risk [...].“ (Smithson und Song 2004, S.58)

Im Rahmen von Basel II wird dieses Modell unter bestimmten qualitativen und quantitativen Vorgaben zugelassen (vgl. Kapitel 2.2.4). In diesem Fall wird der Bank eingeräumt, die regulatorischen Eigenkapitalanforderungen über geeignete Risikomaße aus einer Verlustverteilung zu berechnen (vgl. Basel II, Tz.655). Im Rahmen der Basler Vorgaben werden Methoden skizziert, die Bestandteil dieses fortgeschrittenen Messansatzes sein müssen. Diese umfassen qualitative Aspekte, interne und externe Verlustdatensammlungen, die Berücksichtigung extremer Verluste sowie die Einbeziehung interner und externer Einflussfaktoren. In den folgenden Abschnitten werden qualitative Erhebungen über Self-Assessments, die Sammlungen von Schadensfällen über Verlustdatenbanken, die Erweiterung durch die Extremwerttheorie sowie die Einbindung von Indikatormodellen dargestellt. Dieses erfolgt vor dem Hintergrund der Quantifizierung operationeller Technologierisiken mittels einer Verlustverteilung.

a Self-Assessment

Eine ausschließlich quantitative Erfassung operationeller Risiken ist in Teilen nur schwer möglich, so dass Verlusthöhe und -häufigkeit dann nur qualitativ geschätzt werden können. Somit stellt schlicht die Nichtverfügbarkeit von Al-

ternativen einen Grund für den Einsatz qualitativer Methoden dar. Ein weiteres Argument ist, dass bei einem vollständigen Verzicht auf Meinungen interner Mitarbeiter oder externer Experten wichtiges Wissen verloren geht. Eine Möglichkeit zur Erhebung dieser Einschätzungen ist das Self-Assessment. Auch aus den genannten Gründen stellen Self-Assessments Stand heute die mit am häufigsten eingesetzte Methode zum Management operationeller Risiken dar:

„Self-Assessment routines are probably the most common tool in use today to adress operational risk.“ (Sampson 2004, S.71)

Ein Self-Assessment umfasst in der Phase der Risikoquantifizierung im Wesentlichen die Einschätzung von Eintrittswahrscheinlichkeiten und Verlusthöhen.

Self-Assessments können zum Beispiel über moderierte Workshops oder direkte Interviews durchgeführt werden. Hierbei werden Einflussgrößen des Risikoumfelds in einem Workshop oder mittels strukturierter Fragebögen erhoben. Entscheidend für den Erfolg der Methode ist der Entwurf der richtigen Fragestellungen, um systematische Verzerrungen zu verhindern (vgl. Ebnöther et al. 2002, S.5):

- Direkte Fragen nach Eintrittswahrscheinlichkeiten oder Verlusthöhen sind nach Möglichkeit zu vermeiden.
- Komplexe Zusammenhänge sollten im besten Fall ausschließlich über das Modell abgeleitet werden, so dass die Expertenschätzungen sich auf möglichst simple Sachverhalte beziehen können.
- Die Fragen sollten anreizkompatibel (z.B. im Hinblick auf die ausgeübte Position des befragten Mitarbeiters) konstruiert sein und darüber hinaus eine Möglichkeit zur wechselseitigen Kontrolle der Antworten vorsehen.

Im Rahmen der Expertenbefragungen können auch Risikoszenarien entworfen werden, die versuchen, zukünftiges Verlustpotential zu schätzen. In der Regel sind die qualitativen Einschätzungen jedoch nicht ausreichend und müssen mit quantitativen Daten kombiniert werden. In der Praxis eignet sich dafür die Technik der bayesianischen Schätzung (vgl. Alexander 2003, S.137ff.). Hierdurch können aus Expertenmeinungen geschätzte Verteilungen mit internen oder externen Daten zu einer gemeinsamen Verteilung kombiniert und somit beides berücksichtigt werden.

Das Self-Assessment ist in starkem Maße abhängig von der Gestaltung der Erhebung, beispielsweise durch die Auswahl der richtigen Experten und Fragen und einer zielführenden Organisation der Befragungen. Über das Wissen der IT-Experten kann das in der Bank vorhandene Verständnis technologischer Risiken genutzt werden, um die Zusammenhänge und Strukturen zu erkennen. Dabei ist

neben den Experten auch die Dokumentation der IT-Umgebung relevant. Der zugrunde liegende Risikobegriff ist jedoch stets institutsspezifisch. Durch regelmäßige Wiederholung des Self-Assessments oder durch Aktualisierung der Szenarien kann der Dynamik des Risikoumfelds Rechnung getragen werden.

Die zentrale Kritik an qualitativen Methoden wie dem Self-Assessment, ist die in einem hohen Maß vorhandene Subjektivität (Sampson 2004, S.71). Insbesondere bei durch indirekte Fragen ermittelten Annahmen über die Häufigkeit und Höhe von Verlusten, sind Abgleiche mit empirischen Daten vorzunehmen. Die Risikosensitivität hängt stark von der Qualität der Fragestellung und deren inhaltlichem Bezug zur Risikosituation ab (vgl. Faisst und Kovacs 2003, S.345). Hier existiert jedoch gerade im Bereich der Informationstechnologie durch eine effektive Nutzung des Expertenwissens ein gewisses Potential.

b Verlustdatenbank

Einen wichtigen Bestandteil eines profunden Risikomanagements stellt die Verbindung des gewählten Modells mit den in der Realität auftretenden Schäden dar. Hierzu schreibt Basel II für die fortgeschrittenen Messansätze die regelmäßige Erfassung interner Verlustdaten vor (vgl. Basel II, Tz.670ff.). Als Instrument zur strukturierten Sammlung dieser Daten bietet sich eine Verlustdatenbank an. Eine solche Datenbank verwaltet Informationen über die vollständige Verlusthistorie des Kreditinstitutes, unabhängig von einzelnen Organisationseinheiten oder bestimmten Risikokategorien (vgl. Röckle 2002, S.110).

Schadensdaten dienen als Ausgangsbasis des sogenannten Verlustverteilungsansatzes, bei dem aus empirischen Daten eine Verteilung der Häufigkeit sowie der Höhe der Verluste ermittelt wird (vgl. Frachot, Georges und Roncalli 2001, S.2). Diese Informationen können retrograd aus den Verlustdatenbanken ermittelt werden. Falls ausreichend Daten vorhanden sind, kann die Verlusthöhe oder -häufigkeit direkt in Form einer diskreten Verteilung modelliert werden (vgl. Röckle 2002, S.110). Alternativ können Verlustdaten dazu genutzt werden, für bestimmte Verlustverteilungen die Parameter zu schätzen (vgl. Ebnöther et al. 2002, S.7f.). Bei dieser Methode wird die Wahrscheinlichkeitsverteilung ex ante vorgegeben und parametrisiert. Hierüber können Bereiche, für die nur wenige Daten vorliegen, extrapoliert werden. Für die parametrische Methode muss nicht zwangsläufig nur eine Verteilung gewählt werden, es kann für die Verlusthöhe zum Beispiel eine Lognormal- oder Beta-Verteilung mit der generalisierten Pareto-Verteilung (GPD) kombiniert werden (vgl. Ebnöther et al. 2002,

S.8). Analog können auch die Eintrittswahrscheinlichkeiten für Verlustereignisse modelliert werden. Auch hierfür stehen empirische oder parametrische Verteilungen zur Verfügung (vgl. Röckle 2002, S.113f.).

Um die Überprüfbarkeit im Rahmen der zweiten Säule der Basler Verordnung zu ermöglichen, müssen Kreditinstitute Verlustdaten entsprechend einem vorgegebenen Schema erfassen (vgl. Basel II, Tz.673). Die einzelnen Verluste müssen den in Kapitel 2.2.1 beschriebenen Geschäftsfeldern zugeordnet werden (vgl. Basel II, Anhang 8). Darüber hinaus ist es gefordert, die Entstehung der Verluste auf primäre und sekundäre Kategorien von Verlustereignissen abzubilden (vgl. Basel II, Anhang 9).

Zusätzlich zu internen Verlustdatenbanken ist es sinnvoll, diese mit externen Daten zu ergänzen. Als externe Daten werden zum Beispiel Veröffentlichungen, Studien sowie Datenpools angesehen, die die Verlustdaten unterschiedlicher Kreditinstitute zusammenführen (vgl. Röckle 2002, S.84f.). Die Basler Richtlinie schreibt auch die Verwendung externer Daten vor. Hierüber sollen besonders schwere Verluste berücksichtigt werden, die gegebenenfalls im spezifischen Kreditinstitut noch nicht aufgetreten sind (vgl. Basel II, Tz.674). Hierbei ist jedoch zu beachten, dass externe Daten in der Regel Verluste überschätzen (siehe Fontnouvelle et al. 2003) und gewichtet mit den eigenen Daten kombiniert werden müssen.

Zur Vorbereitung der Basel-II-Einführung wurden Erhebungen über das Ausmaß des operationellen Risikopotentials durchgeführt. Im Rahmen der Loss Data Collection Exercise 2002 (LDCE) wurden Verlustdaten von 89 internationalen Banken für das Jahr 2001 erhoben (siehe BCBS 2003c). Die Daten aus dieser Studie wurden auf mögliche zugrunde liegende Verteilungen untersucht. In der Regel stellen Verteilungen mit ausgeprägten Rändern, wie zum Beispiel die Burr-, Loggamma- oder die Pareto-Verteilung eine gute Näherung der hohen Verluste dar (vgl. Fontnouvelle und Rosengren 2004, S.13). Betrachtet man das gesamte Spektrum der Verluste, können teilweise auch Verteilungen mit einem mittelmäßig ausgeprägten Rand, wie zum Beispiel die Lognormal-Verteilung verwendet werden (siehe Moscadelli 2004). Im Randbereich kann das Modell durch die GPD noch verbessert werden. Die Häufigkeitsverteilung kann durch die Poisson- oder die negative Binomial-Verteilung angenähert werden (vgl. Fontnouvelle und Rosengren 2004, S.22ff.).

Bei der Untersuchung wurde keine Unterscheidung hinsichtlich der Kategorien operationeller Risiken (Prozess-, Human-, Technologie-, externe Risiken) getroffen. Sämtliche Aussagen beziehen sich auf die definierten Kategorien von Verlustereignissen. Für die Technologierisiken spielen die Verlustereignisse aus externen betrügerischen Handlungen (Teilkategorie Systemsicherheit), aus Ge-

schäftsunterbrechung und Systemausfällen (alle Teilkategorien) und aus Abwicklung, Lieferung und Prozessmanagement (Teilkategorie Erfassung, Abwicklung und Betreuung von Transaktionen) eine Rolle. Tabelle 4.4 stellt die Anteile der den Technologierisiken zuzurechnenden Verluste nach der LDCE 2002 zusammen:

Ebene 1	**Ebene 2**	**Anzahl**	**Wert**
Externe betrügerische Handlungen	Systemsicherheit	0,14%	0,28%
Geschäftsunterbrechung und Systemausfälle	–	1,14%	2,73%
Abwicklung, Lieferung und Prozessmanagement	Erfassung, Abwicklung und Betreuung von Transaktionen	23,78%	22,08%
∑ Summe		25,06%	25,09%

Tabelle 4.4: Anteile der Technologierisiken
(vgl. BCBS 2003c, S.9)

Die Ereignisse der Teilkategorie Systemsicherheit spielen hier keine wesentliche Rolle. Geschäftsunterbrechung und Systemausfälle treten selten auf, haben aber einen vergleichsweise hohen durchschnittlichen Verlust pro Ereignis. Die Erfassung, Abwicklung und Betreuung von Transaktionen machen den Großteil der Verluste im Bereich der Technologierisiken aus.

Den Verlustdatenbanken liegt aufgrund der in Basel II geforderten Einteilung in Geschäftsfelder und Ereignistypen bereits ein einfaches Verständnis von Technologierisiken und der Struktur des Kreditinstitutes zugrunde. Über eine weitere Detaillierung der relevanten Kategorien kann ein genaueres Modell aufgebaut werden. Ein gewichtiger Nachteil von Verlustdatenbanken ist die indirekte Annahme einer unveränderten Kausalstruktur (vgl. Röckle 2002, S.120). Durch die vergangenheitsbezogene Sicht wird auf dynamische Veränderungen nur verzögert reagiert. Insbesondere große Schäden haben aber oft eine Anpassung des technologischen Umfelds zur Folge.

Die gemessenen Risiken haben bedingt durch die starre Systematik ein hohes Maß an Objektivität. Aufgrund von Problemen bei der Erfassung und den nachweislichen Tendenzen externer Daten, ist die Risikosensitivität kritisch zu hinterfragen.

c Extremwerttheorie

Eine wesentliche Herausforderung des Risikomanagements stellen sogenannte Ausnahmeverluste dar, die selten auftreten, jedoch ein hohes Ausmaß annehmen. Klassische Verlustverteilungen unterschätzen diese Extreme häufig. Zur Modellierung der Ausnahmeverluste im Risikomanagement wird die Extremwerttheorie eingesetzt (siehe Embrechts, Klüppelberg und Mikosch 1997). Formal wird darunter die Verteilung der Maxima oder die Verteilung der Werte oberhalb eines Schwellenwertes verstanden.

Eine zentrale Aussage der Extremwerttheorie ist das Extremal Types Theorem: Konvergiert die Verteilung der normalisierten Maxima einer Zufallsvariable für infinitesimale Realisationen gegen eine Verteilung, gehört diese zu einer von drei Verteilungen der Extremwerttheorie (vgl. Fisher and Tippet 1928, S.210ff.). Die Weibull-Verteilung repräsentiert dabei Verteilungen mit einem „light tail“, die Gumbel-Verteilung modelliert einen „medium tail“ und die Frechet-Verteilung steht für einen „fat tail“ (vgl. Moscadelli 2004, S.22).

Eine Alternative zur Betrachtung der Maxima einer Verteilung ist die Untersuchung der Verteilung aller Ausprägungen x oberhalb eines Schwellenwertes. Diese kann für eine große Anzahl an Verteilungsfunktionen entsprechend dem Theorem von Pickands, Balkema und de Haan gut durch die zweiparametrige generalisierte Pareto-Verteilung angenähert werden. Hierbei stellen die Parameter ξ die Form (shape) und β den Maßstab (scale) der Verteilung dar (vgl. McNeil 2000, S.6).

$$GPD_{\xi\beta}(x) = \begin{cases} 1-\left(1+\xi\frac{x}{\beta}\right)^{-1/\xi} & \text{für } \xi \neq 0 \\ 1-e^{-x/\beta} & \text{für } \xi = 0 \end{cases} \tag{4.2}$$

Es gilt $\beta > 0$ und $x \geq 0$ für $\xi \geq 0$ sowie $0 \leq x \leq -\beta/\xi$ für $\xi < 0$. Mittels dieser Verteilungsfunktion können die empirischen Daten oberhalb eines Schwellenwertes extrapoliert und somit durch die verwendeten Risikomaße (vgl. Kapitel 2.1.3) besser berücksichtigt werden. Eine Vorhersage extremer Verluste kann hierüber aber sicherlich nicht erfolgen (vgl. Embrechts, Furrer und Kaufmann 2003, S.246). Problematisch bei der Anwendung der Extremwerttheorie ist die Schätzung eines geeigneten Schwellenwertes. Zum einen sollte dieser möglichst hoch gewählt werden, da die GPD nur im Randbereich der Verteilung Gültigkeit besitzt, zum anderen müssen jedoch ausreichend Daten zur Parametrisierung der GPD vorliegen. Die Schätzung der Schwelle erfolgt in der Regel graphisch

durch die „Sample Mean Excess Loss“-Funktion. Die Schätzung der Parameter ξ und β wird dann beispielsweise über die „Maximum Likelihood“-Methode vorgenommen (vgl. McNeil und Saladin 1997, S.5ff.).

Untersuchungen der Daten aus der LDCE 2002 ergeben, dass beispielsweise die Verteilungen der Verluste aus der Kategorie Abwicklung, Lieferung und Prozessmanagement extreme Ränder aufweisen können (vgl. Fontnouvelle und Rosengren 2004, S.15).

Die Extremwerttheorie hat jedoch weder einen inhaltlichen Bezug zu einem allgemeinen Verständnis operationeller Technologierisiken noch zu den jeweiligen bankspezifischen Strukturen. Eine Reaktion auf Veränderungen in der Risikosituation erfolgt nur zeitversetzt über die veränderte Datengrundlage. Die Extremwerttheorie sollte damit als ein Bestandteil des auf der Modellierung einer Verlustverteilung basierenden Risikomanagements betrachtet werden.

Die Extremwerttheorie kann grundsätzlich als eine objektive Methode zur Quantifizierung angesehen werden. Einzig die individuelle Wahl des Schwellenwertes sollte nachvollziehbar begründet werden. Die Risikosensitivität ist stark vom Umfang der erhobenen Daten abhängig. Insbesondere müssen ausreichend Werte oberhalb des Schwellenwertes vorliegen. Bei der Ermittlung der Risikomaße ist ferner die hohe Sensitivität gegenüber den Verteilungsparametern zu berücksichtigen (vgl. Moscadelli 2004, S.69).

d Indikatoransatz

Die Risiken, denen Banken ausgesetzt sind, sind nicht statisch und unterliegen ständigen Veränderungen über die Zeit (vgl. Braun 1984, S.66). Daher werden Frühwarnsysteme eingesetzt, um diese zukünftigen Entwicklungen möglichst gut zu antizipieren. Sie basieren im Kern auf Indikatoren, die als Anzeichen für potentielle Veränderungen im Risikoumfeld interpretiert werden. Über die Analyse solcher risikorelevanter Größen können Rückschlüsse über das Ausmaß und die Verlusterwartung der entsprechenden Risiken gezogen werden (vgl. Piaz 2002, S.152). Als Indikatoren können sowohl quantitative Größen als auch qualitative Einschätzungen dienen. Um ein effizientes Frühwarnsystem zu implementieren, müssen die Indikatoren zumindest die Kriterien der Eindeutigkeit, Frühzeitigkeit, rechtzeitigen Verfügbarkeit, vollständigen Abdeckung und ökonomischen Vertretbarkeit erfüllen (vgl. Krystek und Müller 1999, S.179 oder Martin und Bär 2002, S.112f).

Im Zusammenhang mit Technologierisiken steht eine Vielzahl sowohl technischer als auch fachlicher Indikatoren zur Verfügung. Nachfolgend werden beispielhaft einige gängige Risikoindikatoren aufgelistet (siehe Münchbach 2001; Minz 2004):

- Anzahl der Anwendungssysteme
- Anzahl der bestehenden Schnittstellen
- Alter der Anwendungssysteme
- Systemverfügbarkeit und Auslastung
- Grad der Qualifikation der IT-Mitarbeiter

Um möglichst frühzeitig Informationen über Änderungen im Risikopotential zu erhalten, können Indikatoren wie die Systemverfügbarkeit oder Auslastung automatisiert gemessen werden. Tendenziell qualitative Indikatoren, wie beispielsweise die Qualifikation der IT-Mitarbeiter, müssen regelmäßig erhoben werden.

Die Betrachtung von Risikoindikatoren kann das Risikobewusstsein stärken und so implizit das Verständnis der Technologierisiken verbessern. Auch wenn die Strukturen innerhalb der Bank nur eingeschränkt berücksichtigt werden, können über diesen Ansatz IT-Mitarbeiter für bestimmte Zusammenhänge sensibilisiert werden. Ein explizites Modell operationeller Technologierisiken liegt dieser Methode nicht zugrunde. Indikatoransätze stellen jedoch eine Alternative dar, zukünftige Veränderungen in der Risikosituation zu antizipieren.

In der Regel werden Indikatoransätze auf bankintern festgelegten Größen basieren, so dass nur ein geringer Grad an Objektivität gegeben ist. Der kausale Zusammenhang zwischen den Risiken und den einzelnen Indikatoren ist in der Regel nur ex post feststellbar. Aus diesem Grund ist die Risikosensitivität der Indikatoransätze nur schwer nachzuweisen.

4.2.3 Modell funktionaler Abhängigkeiten

Methoden, die indirekt auf einem Modell des Unternehmens basieren, zielen auf eine Offenlegung sowohl der Risiken als auch der Zusammenhänge ab. Hierzu wird vorgeschlagen, die wesentlichen Prozesse einer Bank als Graph zu modellieren (vgl. Ebnöther et al. 2002, S.5f.). Die Knoten repräsentieren dabei die jeweiligen Prozesselemente (z.B. Anwendungssysteme), an welchen Fehler auftreten können, die Kanten verkörpern bestehende Abhängigkeiten. Unterschiedliche Risikofaktoren (z.B. Hardwarefehler) wirken an den Knoten und generieren zufällige Verluste. Der stochastische Summenprozess der einzelnen Verlus-

te quantifiziert das gesamte finanzielle Risikopotential. Entscheidend ist, dass die Quantifizierung der Risiken auf einem Unternehmensmodell der Bank beruht, welches die zu betrachtenden Elemente und Strukturen enthält. Hierfür werden direkte, funktionale Abhängigkeiten betrachtet. In den folgenden Absätzen werden die ursprünglichen Ansätze nach Kühn und Neu (2003) sowie Leippold und Vanini (2003) beziehungsweise die nachfolgenden Quellen entsprechend Kühn und Neu (2004) sowie Leippold und Vanini (2005) berücksichtigt.

Kühn und Neu definieren den Begriff OR-Prozess zur Beschreibung der Komponenten (Prozess, Human, Technologie oder externe Ereignisse), die operationelle Risiken auslösen können (vgl. Kühn und Neu 2003, S.651). Der Ausfall eines solchen OR-Prozesses stellt in diesem Sinne ein Risikoereignis dar. Konkret wird bei Kühn und Neu ein diskretes Modell mit zwei Zuständen (up/down) je OR-Prozess unterstellt. Zwischen diesen OR-Prozessen werden nun direkte funktionale Abhängigkeiten betrachtet. Der Zustand *n* jedes OR-Prozesses *i* wird über die Unterstützungsfunktion h_i ermittelt, die angibt, wieviel Unterstützung durch andere benötigte OR-Prozesse und weitere Einflussgrößen geleistet wird (vgl. Kühn und Neu 2003, S.656):

$$h_i(t) = \vartheta_i - \sum_j \omega_{ij} n_j(t) + \eta_i(t) \tag{4.3}$$

Ausgangspunkt ist die durchschnittliche Unterstützung ϑ_i, die eine voll funktionsfähige Umgebung zur Verfügung stellt. Das Gewicht ω_{ij} drückt den Grad der funktionalen Abhängigkeit des OR-Prozesses *i* vom OR-Prozess *j* aus.

Exogene Zustandsveränderungen werden über η_i, bestehend aus allgemeinen, gewichteten Risikofaktoren Y_k (z.B. Stromausfälle) und einem skalierten idiosynkratischen Faktor ϵ, abgebildet (vgl. Kühn und Neu 2004, S.5):

$$\eta_i(t) = \sum_{k=1}^{K} \beta_{ik} Y_k(t) + \xi_i \epsilon_i(t) \tag{4.4}$$

Im hier betrachteten Modell wird sowohl für die allgemeinen Risikofaktoren als auch für den idiosynkratischen Faktor eine Standardnormal-Verteilung unterstellt.

Die Zustandsänderung eines OR-Prozesses ergibt sich aus einer Abbildung der Unterstützungsfunktion auf den Wertebereich der Zustände (up/down).

$$n_i(t+\Delta t) = \Theta(-h_i(t)) \tag{4.5}$$

Diese Normierung erfolgt numerisch mittels einer Step-Funktion Θ auf die Werte {0;1}. Diese ist wie folgt definiert:

$$\Theta(x) = \begin{cases} 1 & \text{für } x \geq 0 \\ 0 & \text{für } x < 0 \end{cases} \tag{4.6}$$

Auf das Modell der OR-Prozesse bezogen bedeutet dies, dass der OR-Prozess ausfällt, sobald die geleistete Unterstützung unter einen bestimmten Schwellenwert sinkt. Die Regeneration erfolgt jeweils innerhalb von Δt.

Die finanziellen Verluste werden über prozessspezifische Verlustverteilungen modelliert. Dabei sind die einzelnen Zufallsvariablen voneinander unabhängig. Die Ermittlung des Risikopotentials erfolgt über die Summierung der einzelnen Verluste und ist somit getrennt von der Darstellung der Prozesszustände (vgl. Kühn und Neu 2004, S.6).

Das bisher beschriebene Modell wird durch Leippold und Vanini in mehreren Punkten erweitert (vgl. Leippold und Vanini 2003, S.2f.). Einerseits werden die finanziellen Verluste in Beziehung zur Wertkette gesetzt und mögliche Kosten in das Modell integriert. Darüberhinaus werden pfadabhängige Gegenmaßnahmen betrachtet. Andererseits wird das Modell direkter, funktionaler Abhängigkeiten formal mittels eines Graphen abgebildet. Grundlage der Betrachtung stellen bei Leippold und Vanini die „operational risk assets“, kurz Asset, dar:

„Assume (a) a directed graph, (b) risk factors X and Y defined on a suitable probability space, (c) the fixed and stochastic cost components, and (d) the set of performance and node work flows. [...] An operational risk asset consists of all the objects (a) through (d).“ (Leippold und Vanini 2005, S.65)

Je Asset wird genau ein Zustand betrachtet, dessen Wertebereich stetig ist und im Intervall [0,1] liegt. Die Ermittlung der Zustandsveränderung erfolgt bei Leippold und Vanini ebenso über die von anderen Assets und Risikofaktoren geleistete Unterstützung. Die Supportfunktion ist hier jedoch stetig definiert.

$$dh_i = s_i(h_i)(b_i(h_i) - (w \circ f(h))_i)\,dt - \sigma_i\,dW_i - \varsigma_i\,dZ \tag{4.7}$$

Der Term $b_i(h_i)$ bezeichnet die durchschnittliche Unterstützung eines funktionsfähigen Graphen, $s_i(h_i)$ (Speed-Funktion) stellt die Geschwindigkeit der Zustandsänderungen dar. Die Regeneration ist variabel und erfolgt nicht innerhalb eines festen Zeitintervalls. Die Supportfunktion umfasst ferner zum einen die gewichteten topologischen Abhängigkeiten von anderen Assets $(w \circ f(h))_i$, zum anderen werden die Einflüsse der operationellen Risikofaktoren $\sigma_i dW_i$ und eines externen Risikofaktors $\varsigma_i dZ$ gewichtet berücksichtigt.

Die Normierung auf den Wertebereich der Zustände erfolgt hier über die complementary error function (*erfc/2*), wodurch die Betrachtung von Kühn und Neu auf Zwischenzustände erweitert wird (vgl. Leippold und Vanini 2003, S.7f.).

Die wesentlichen Artefakte beider Modelle sowie bestehende Unterschiede sind in Tabelle 4.5 zusammengefasst.

Komponenten	**Kühn und Neu**	**Leippold und Vanini**
Elemente	**OR-Prozess**	**Operational risk asset**
Wertebereich des Zustands	Diskret {0,1}, Step-Funktion	Stetig [0,1], *erfc*/2
Betrachtetes Zeitintervall	Δt	Stetig
Zeitabhängigkeit	Bezug über $t+\Delta t$	Stetig, *dt*
Regeneration	Direkt in Δt	Speed function
Risikofaktoren	**Common risk factors**	**Operational risk factors**
Betrachtete Zustände	Standardnormal-Verteilung	Brown'sche Bewegung
Externe Störgröße	Standardnormal-Verteilung	Brown'sche Bewegung
Verluste	**Unabhängige Verluste**	**Cost- und Loss function**
Wertebereich	Lognormal-Verteilung	Zufallsvariable V_{ip}
Verknüpfung	Unabhängig	Dauer und Schwere
Ermittlung Verlustverteilung	**Simulation**	**Simulation**
Zeitintervall	Δt = 1 Tag	Stetig
Zeitraum	T = 1 Jahr = 365 Tage	Beispielhaft 30 Tage

Tabelle 4.5: Vergleich der Modelle funktionaler Abhängigkeiten

Das Verständnis der konkreten Risikosituation in der Bank wird durch die Modellierung der Elemente sowie bestehender Abhängigkeiten wesentlich unterstützt. Die Struktur des Kreditinstitutes sowie dynamische Veränderungen am Aufbau oder Ablauf können im Modell nachvollzogen werden. In den bestehenden Methoden ist ein Bezug zu einer expliziten Definition der Technologierisiken möglich, jedoch nicht enthalten.

Eine analytische Ermittlung der Verlustverteilung ist in der Regel nicht möglich. Hierzu wird in beiden Ansätzen eine Monte-Carlo-Simulation eingesetzt. Die Simulation erlaubt grundsätzlich die Generierung beliebig umfangreicher Daten. Hierzu müssen jedoch sämtliche Parameter über Annahmen von Exper-

ten oder empirische Ergebnisse geschätzt werden. Je mehr Parameter im Modell funktionaler Abhängigkeiten explizit gesetzt werden müssen, desto komplexer wird diese Schätzung. In diesem Zusammenhang stellt besonders das stetige Modell von Leippold und Vanini (vgl. Formel 4.7) hohe Anforderungen an die Parametrisierung. Durch die Möglichkeit, das Risikoumfeld der Bank direkt zu modellieren, weist die Methode eine hohe Risikosensitivität auf.

4.2.4 Kritischer Vergleich

Die dargestellten Methoden tragen in unterschiedlicher Weise zur Erreichung der beiden zentralen Ziele dieser Arbeit bei (vgl. Tabelle 4.6). Keine der Methoden erfüllt die aufgestellten Kriterien in vollem Umfang. Insbesondere die Schaffung eines Begriffsverständnisses wird nur unzureichend unterstützt.

Zentrale Ziele	**Verständnis**			**Quantifizierung**	
Kriterien	**Begriff**	**Struktur**	**Dynamik**	**Objektivität**	**Sensitivität**
Standardansatz	-	-	+/-	+/-	+/-
Self-Assessment	+/-	+	+/-	-	+/-
Verlustdatenbank	+/-	+/-	-	+	+/-
Extremwerttheorie	-	-	-	+	+/-
Indikatormodell	+/-	+/-	+	-	-
Modell funktionaler Abhängigkeiten	+/-	+	+	+/-	+

Tabelle 4.6: Vergleich der dargestellten Methoden
(unterstützt (+), neutral (+/-), eingeschränkt (-))

Der Nachteil des ersten Modells, Risiken über beeinflussende Größen abzuschätzen, liegt in einem fehlenden Risikobewusstsein. Es ist nicht geeignet, ein Verständnis für die Zusammenhänge und Strukturen operationeller Technologierisiken zu schaffen. Vorteilhaft ist die Möglichkeit der einfachen Quantifizierung. Dies ist jedoch mit einer Reduktion der Risikosensitivität verbunden.

Betrachtet man das auf einer Verlustverteilung basierende Modell als wirkungsvolle Verbindung der vier genannten Methoden, ergibt sich eine deutlich bessere Abdeckung der Zielkriterien. Als gewichtiger Nachteil kann aber die hohe Stationarität angesehen werden, wodurch strukturelle Änderungen als Folge immenser Verluste nur zeitverzögert berücksichtigt werden (vgl. Embrechts, Furrer und Kaufmann 2003, S.15). Ferner liegt auch diesem Modell kein explizites Begriffsverständnis operationeller Technologierisiken zugrunde.

Das Modell funktionaler Abhängigkeiten stellt eine effektive Erweiterung der obigen Modelle dar. In Verbindung mit einem expliziten Verständnis der Begriffe und Zusammenhänge operationeller Technologierisiken, besäße dieses Modell einen hohen Grad der Zielerreichung. Das zentrale Ergebnis des Modellvergleichs ist es daher, das Modell funktionaler Abhängigkeiten im diskreten Fall (vgl. Formel 4.3) mit der Technologierisiko-Ontologie aus Kapitel 3.2 zu verbinden, um die verbleibenden Schwächen zu eliminieren.

4.3 Ontologie-zentrierte Simulation

In Kapitel 3 wurde gezeigt, dass durch den Einsatz von Ontologien zur wissensbasierten Modellierung das Verständnis technologischer Risiken gefördert werden kann. Formale Ontologien können ebenso verwendet werden, um bei der Entwicklung von Simulationsmodellen die semantische Lücke zwischen der technischen und der fachlichen Perspektive zu schließen (vgl. Cuske, Dickopp und Seedorf 2005, S.84). Im Rahmen dieser Arbeit wird der Ansatz einer Ontologie-zentrierten Simulation gewählt, um die in Kapitel 3 dargestellten Vorteile eines expliziten Verständnisses in die Phase der Quantifizierung zu übertragen. Grundlage der entwickelten Methode zur Quantifizierung stellt daher die Technologierisiko-Ontologie dar. Diese wird in ein Simulationsmodell transformiert, das sich wesentlich auf das in Kapitel 4.2.3 vorgestellte Modell funktionaler Abhängigkeiten stützt. Als Eckpfeiler dieses Modells werden die Anwendungssysteme (*Asset*), ihre Eigenschaften der Ordnungsmäßigkeit sowie die bestehenden wechselseitigen Beziehungen betrachtet. Die Ursachen für Systemausfälle liegen zum einen in den definierten Abhängigkeiten zu anderen Anwendungssystemen, zum anderen werden die Einflüsse unterstützender IT-Komponenten und Aufgaben des IT-Managements als Risikofaktoren interpretiert. Die Ermittlung des Risikopotentials erfolgt über die Auswirkungen auf die Aktivitäten der Wertkette und die damit verknüpften finanziellen Effekte als Verlustfunktion.

Ziel der Transformation ist ein Simulationsmodell bestehend aus Elementen, Inputs und Outputs (vgl. Kapitel 2.3.3). Dazu werden die in der Technologierisiko-Ontologie enthaltenen Konzepte erst auf die wesentlichen Konzepte

des Modells funktionaler Abhängigkeiten überführt. In einem zweiten Schritt werden die Assets und ihre Eigenschaften auf Elemente, die Risikofaktoren auf Input-Größen und die Verlustfunktionen auf Output-Größen projiziert. Für die Darstellung der Transformation des Technologierisiko-Modells in das Simulationsmodell wird entsprechend Kapitel 3.2 die Description Logic verwendet. Die Grundlage für die Simulation stellt ein stochastischer Summenprozess dar.

4.3.1 Zentrale Elemente des technologischen Umfelds

Für das zu entwickelnde Modell zur Quantifizierung von Technologierisiken stellen die Anwendungssysteme von Banken den wesentlichen Gegenstand der Betrachtung dar. Diese Besonderheit resultiert einerseits aus der wichtigen Aufgabe, die den Anwendungssystemen über die funktionale Unterstützung der Aktivitäten (*operate*) im Rahmen der Wertkette zukommt. Andererseits hebt das Basler Verständnis operationeller Risiken die Bedeutung dieser Systeme hervor. Die Anwendungssysteme und ihre Eigenschaften gelten im Rahmen dieser Arbeit als zentrale Verursacher operationeller Technologierisiken. Operationelle Risiken können als ein Graph wesentlicher operativer Aktivitäten und unterstützender Anwendungssysteme aufgefasst werden (vgl. Leippold und Vanini 2005, S.61ff.). Diese formale Herangehensweise wird hier aufgegriffen und für das in Kapitel 3 entwickelte Verständnis von Technologierisiken konkretisiert.

Die Anwendungssysteme (*ApplicationSystem*) und ihre Abhängigkeiten (*depend*) formen hierzu den gerichteten Graphen. Dieser ist die Grundlage für die wesentlichen Elemente des technologischen Umfelds (*Asset*).

$$Asset \equiv ApplicationSystem \tag{4.8}$$

Charakteristisch für jedes Anwendungssystem ist der Bezug zu den Aktivitäten der Wertkette. Hierdurch ist es möglich, die Anwendungssysteme allgemein nach Aktivitäten zu unterscheiden. So können Systeme zur Unterstützung des Vertriebs, der Auftragsabwicklung oder des Rechnungswesens betrieben werden. Im Speziellen sind die Anwendungssysteme für konkrete Geschäftsbereiche einzugrenzen. Für den Geschäftsbereich Handel (nach Basel II) sind beispielsweise eine Handelsplattform oder ein Abwicklungssystem vorstellbar.

Verantwortlich für die möglichen Verluste sind die Zustände (*State*) der betrachteten Ressourcen des Technologieumfelds. Diese werden mittels der risikorelevanten Eigenschaften (*Property*) in das Modell integriert.

$$State \equiv Property \tag{4.9}$$

So wird im Unterschied zu den Modellen funktionaler Abhängigkeiten (vgl. Kapitel 4.2.3) mehr als ein Zustand je Ressource unterschieden. Für die Anwendungssysteme werden die Zustände Vollständigkeit, Richtigkeit und Zeitgerechtheit modelliert. Der über die Anwendungssysteme definierte Graph stellt die Ausgangsbasis des Simulationsmodells dar. Um die Technologierisiko-Ontologie in das Simulationsmodell zu überführen, werden zunächst die Zustände der Anwendungssysteme in Elemente der Simulation (*Element*) transformiert.

$$Element \equiv State \; \forall \; exhibit \,.\, Asset \tag{4.10}$$

Die Vorgehensweise zur Berechnung wird pro *Element* im Modell textlich (*String*) als mathematische Formel (*formula*) erfasst.

$$\geqslant 1 \; (\; formula \,.\, String \;) \sqsubseteq Element \tag{4.11}$$

Die Ermittlung der Zustandswerte der *formula* erfolgt in Anlehnung an die in Kapitel 4.2.3 dargestellten Modelle funktionaler Abhängigkeiten.

4.3.2 Anwendung der Supportfunktion

Im Rahmen dieser Arbeit wird für die Supportfunktion die diskrete Darstellung entsprechend Kühn und Neu verwendet. Der Operator Θ bezeichnet demnach eine Step-Funktion entsprechend Formel 4.6. Die Werte *n* der Zustände *e* eines Assets *i* hängen zum einen von den Zuständen *s* der beeinflussenden Anwendungssystemen *j* ab, zum anderen sind exogene Einflüsse, dargestellt durch den Term η, verantwortlich für mögliche Störungen. Der Wertebereich der Zustände wird auf gegeben oder nicht gegeben abgebildet, das entspricht numerisch den Werten 0 beziehungsweise 1 (vgl. Kühn und Neu 2003, S.656f.).

$$n_i^e(t) = \Theta \left(-\vartheta_i^e + \sum_{\substack{Asset\ j \\ State\ s\ von\ j}} \omega_{ij}\, n_j^s(t-\alpha_{ij}\,\Delta t) - \eta_i^e(t-\alpha_i\,\Delta t)\right) \tag{4.12}$$

In Anlehnung an Kühn und Neu (2003) ist das Zeitintervall Δt so gewählt, dass alle Eigenschaften innerhalb dieses Intervalls wiederhergestellt werden können. Zeitspannen für die Wiederherstellung werden im Rahmen dieser Arbeit nicht betrachtet. Der Faktor α bestimmt den zeitlichen Bezug. Für $\alpha = 1$ ermittelt sich der Zustand eines Assets direkt aus den vorangegangenen (t-Δt) Zuständen der Einflussgrößen. Prinzipiell sind aber alle Werte $\alpha \in \mathbb{N}_0$ möglich. Der Wert für ϑ beschreibt die Störanfälligkeit eines Assets. Je geringer der Wert gewählt wird, desto eher führt eine Störung in einem unterstützenden Anwendungssystem oder einem zugehörigen Risikofaktor zu einem Systemausfall. Wird der Wert erhöht, kann hierüber eine zunehmende Fehlertoleranz modelliert werden. Der

Faktor ω repräsentiert den Grad der Abhängigkeit von einem unterstützenden Anwendungssystem, im einfachsten Fall 1. Der Ausdruck η beschreibt die exogenen Einflussgrößen, die sich aus beeinflussenden Risikofaktoren und zusätzlichen Störgrößen zusammensetzen.

$$\eta_i^e(t-\alpha_i \Delta t) = \sum_{\substack{Riskfactor\ k \\ State\ u\ von\ k}} \beta_{ik} Y_k^u(t-\alpha_i \Delta t) + \xi_i \epsilon_i(t-\alpha_i \Delta t) \qquad (4.13)$$

Der Einfluss der Werte *Y* der Zustände *u* der beeinflussenden Risikofaktoren *k* werden über β_{ik} gewichtet. Da jedoch nicht davon ausgegangen werden kann, dass die Risikofaktoren zusammen mit den unterstützenden Anwendungssystemen die Ausfälle vollständig erklären, werden sogenannte Störgrößen oder Noise-Faktoren als verbleibende Unsicherheit in das Modell integriert (vgl. Wallmeier 1997, S.23ff.). Diese sind über den gewichteten (ξ) Standardnormalverteilten Term ϵ enthalten. In den nächsten Schritten werden die fachlichen Aspekte der Risikofaktoren und Verlustfunktionen entwickelt und auf entsprechende Konstrukte im Simulationsmodell abgebildet.

4.3.3 Darstellung der Risikofaktoren

Für die im Rahmen dieser Arbeit vorgestellte Methode haben auch die Risikofaktoren eine zentrale Bedeutung. Als Risikofaktoren werden im Rahmen dieser Arbeit zufallsverteilte Einflussgrößen bezeichnet, die direkt Verluste auslösen können. Diese Sichtweise entspricht folgender Definition eines Risikofaktors:

„[A risk factor is a] causal factor that creates a change in earnings for a change in the factor and has a random uncertainty associated with it.“ (King 2001, S.246)

Dieser Ansatz setzt einen kausalen Zusammenhang zwischen einer Veränderung des Risikofaktors und einem negativen finanziellen Effekt, also einem Verlust, voraus. Der Risikofaktor wird dabei als eine Zufallsvariable interpretiert. Eine Möglichkeit zur Analyse eines unsicheren zukünftigen Verlusts aus einem Objekt ist die Identifikation möglichst aller wesentlichen Einflussfaktoren auf diese Zielgröße. Um den Aufwand zu begrenzen, ist es erforderlich, dass die betrachteten Risikofaktoren auf die wesentlichen Einflussgrößen reduziert werden (vgl. Diggelmann 1999, S.79). Für ein aussagekräftiges und praktikables Risikomodell ist es somit entscheidend, die Anzahl der Risikofaktoren sinnvoll zu beschränken. Zur Ermittlung der Risikofaktoren sind unter anderem zwei Verfahren möglich. Bei der statistischen Faktorenanalyse werden über statistische Verfahren Abhängigkeiten zwischen den Verlusten und den Risikofaktoren er-

mittelt. Ein anderer Ansatz ist die Vorgabe ex ante plausibler Faktoren auf Basis ökonomischer Erwägungen (vgl. Wallmeier 1997, S.27; Albrecht, Maurer und Mayser 1996, S.8). Im Rahmen dieser Arbeit werden die IT-Komponenten sowie die Aufgaben des IT-Managements und ihre kritischen Eigenschaften als Risikofaktoren vorgegeben.

$$Riskfactor \equiv ITComponent \sqcup ITManagementTask \tag{4.14}$$

Die Zuordnung zum jeweiligen *Asset* erfolgt über die Relationen *form* und *influence*. Damit wird eine aus zwei Ebenen bestehende Sichtweise realisiert (vgl. Leippold, Doebli und Vanini 2003, S.7). Die Anwendungssysteme stellen die Schnittstelle zu den Aktivitäten der Wertkette dar. Gleichzeitig repräsentieren die Eigenschaften der Risikofaktoren (z.B. Verfügbarkeit) die stochastischen Eingabeparameter (*Input*) im Sinne des Simulationsmodells.

$$Input \equiv State \; \forall \; exhibit \,.\, Riskfactor \tag{4.15}$$

Zentral für die Bewertung des Risikos auf Basis einzelner Risikofaktoren ist die Korrelation dieser Faktoren. Ohne diese rechnerisch zu ermitteln sind zwei grundsätzliche Annahmen möglich. Eine extreme Sichtweise wäre die vollständige beziehungsweise entgegengesetzte Korrelation. Es kann jedoch vielmehr argumentiert werden, dass die Korrelation im Mittel gegen 0 strebt (vgl. Van den Brink 2003, S.34). Im Modell werden die einzelnen Risikofaktoren daher als unabhängig angesehen (vgl. Kühn und Neu 2004, S.6).

Für die Wertebereiche der Zustände der Risikofaktoren sind unterschiedliche Möglichkeiten, wie zum Beispiel stetige Intervalle oder feste Bereiche, denkbar. Im Rahmen dieser Arbeit können die Zustände der Risikofaktoren ausschließlich die Ausprägung "gegeben" oder "nicht gegeben" annehmen. Dies wird numerisch auf die Werte 0 und 1 abgebildet. Zur Speicherung wird die textliche Darstellung der *formula* auf das Konzept *Input* erweitert.

$$\geqslant 1 \left(formula \,.\, String \right) \sqsubseteq Input \tag{4.16}$$

Dies weicht von der Auffassung gemäß Kühn und Neu ab, wonach die Risikofaktoren eindimensional stetig im Intervall [0,1] aufgefasst werden (vgl. Kühn und Neu 2003, S.656f). Die Zustände der Risikofaktoren folgen direkt einer vorgegebenen diskreten Zufallsvariablen *Y*. Für die Modellierung der Häufigkeit des Eintretens von Risikoereignissen im Bereich operationeller Risiken werden unterschiedliche Verteilungsfunktionen verwendet (vgl. Alexander 2003, S.144f.; Cruz 2002, S.87ff.). Häufig kommt beispielsweise die einpara-

metrische Poisson-Verteilung zum Einsatz. Diese modelliert seltene Ereignisse, welche zufällig aber mit konstanter mittlerer Rate λ auftreten (vgl. Hesse 2003, S.188).

$$Y \sim P(\lambda) \quad \text{mit} \quad P(Y=z) = \frac{(\lambda)^z}{z!}\, e^{-\lambda}, \quad z \in \mathbb{N}_0 \tag{4.17}$$

Alternativ kann die zweiparametrige, negative Binomial-Verteilung zur Modellierung der Zeitintervalle zwischen zwei Schadenereignissen eingesetzt werden.

$$Y \sim NB(r, p) \quad \text{mit} \quad P(Y=z) = \binom{z-1}{r-1}\, p^r\, (1-p)^{z-r}, \quad z = r, r+1, \ldots \tag{4.18}$$

Aufgrund der zwei Parameter *r* und *p* ist die negative Binomial-Verteilung im Vergleich zur Poisson-Verteilung besonders im Randbereich besser geeignet, die empirischen Daten möglichst exakt anzunähern (vgl. Cruz 2002, S.89).

Abschließend wird die zweiparametrige, diskrete Binomial-Verteilung vorgestellt. Diese Verteilung entspricht einem Zufallsexperiment, das *n* Wiederholungen einzelner Experimente mit gleichbleibender Wahrscheinlichkeit *p* darstellt (vgl. Hesse 2003, S.184ff.).

$$Y \sim B(n, p) \quad \text{mit} \quad P(Y=z) = \binom{n}{z}\, p^z\, (1-p)^{n-z}, \quad z = 0, \ldots, n \tag{4.19}$$

Anders formuliert entspricht eine Binomial-verteilte Zufallsvariable der Anzahl der Erfolge bei der n-fachen Wiederholung dieses Experiments. Diese Verteilung kann somit ebenso wie die Poisson- oder negative Binomial-Verteilung zur Schätzung der Häufigkeit eingesetzt werden. Der Erwartungswert sowie die Varianz der Binomial-Verteilung ergeben sich wie folgt:

$$E(Y) = n\,p \quad \text{und} \quad V(Y) = n\,p(1-p) \tag{4.20}$$

Die Verwendung obiger Verteilungen entspricht dem aktuellen Stand der Umsetzung in Banken. Diese verwenden bei den Verlustverteilungsansätzen zur Modellierung der Häufigkeiten im Wesentlichen die Poisson- oder die (negative) Binomial-Verteilung (vgl. Deutsche Bundesbank und BaFin 2005, S.18).

Im hier vorgeschlagenen Modell soll jedoch nicht direkt eine Anzahl der pro Jahr eingetretenen Ereignisse oder ein Zeitintervall zwischen zwei Verlusten abgeschätzt werden. Vielmehr wird eine Größe für die Zustandswerte der Risikofaktoren auf täglicher Basis benötigt, um hieraus den Einfluss auf die Anwendungssysteme abzuleiten. Im Bereich der Messung der Zuverlässigkeit von

Software wird häufig eine Bernoulli-Verteilung verwendet, um die Verarbeitung einer Eingabe als entweder richtig oder falsch zu modellieren (vgl. Singpurwalla and Wilson 1999, S.30f.). Bei dieser Vorgehensweise werden Details ausgeblendet und ausschließlich der Prozess der Verarbeitung und die Korrektheit des Ergebnisses betrachtet. Diesem Ansatz folgend wird eine Bernoulli-Verteilung für die Modellierung der Risikofaktoren aus den Bereichen IT-Komponenten und Aufgaben des IT-Managements angenommen.

Über die Bernoulli-Verteilung wird der tägliche Wert eines Zustands diskret, mit den Werten 0 oder 1, modelliert. So kann auf abstrakte Weise der Einfluss des Risikofaktors dargestellt werden, ohne interne Zusammenhänge zu berücksichtigen. Betrachtet man eine Folge von unabhängigen Bernoulli-Verteilungen, ergibt sich ein Bernoulli-Prozess. Da die Binomial-Verteilung die Anzahl der Erfolge bei n-facher Wiederholung eines Bernoulli-Experiments darstellt, ist über Formel 4.20 auch der Erwartungswert des stochastischen Prozesses gegeben (vgl. Hesse 2003, S.185).

4.3.4 Abbildung der Verlustfunktion

Weiteres zentrales Element des hier vorgestellten Risikomodells ist der in Geldeinheiten gemessene finanzielle Verlust aus operationellen Technologierisiken. Risikobehaftete, finanzielle Effekte werden häufig über Faktormodelle abgebildet. Der finanzielle Effekt ergibt sich dabei als funktionale Abbildung gewichteter Zufallsgrößen. Faktormodelle kommen beispielsweise im Bereich der Marktrisiken zur Schätzung von Renditen oder im Bereich der Kreditrisiken zur Ermittlung von Ausfallwahrscheinlichkeiten zum Einsatz. Da im Bereich operationeller Risiken eine verlustorientierte Betrachtung vorherrscht, findet hier vermehrt der Begriff der Verlustfunktion Verwendung. Diese beschreibt eine funktionale Abbildung der Werte oder Wertveränderungen modellierter Konstrukte (hier *Asset* oder *Riskfactor*) auf einen Betrag pro Risikoposition. Leippold und Vanini grenzen den Begriff der Verlustfunktion noch von der Kostenfunktion ab (vgl. Leippold und Vanini 2005, S.68). Ersterer bezieht sich im engeren Sinn auf Verluste durch verursachte Störungen in der Wertkette, letzterer auf direkte Kosten durch zu treffende Instandhaltungs- oder Gegenmaßnahmen. In dieser Arbeit wird ausschließlich der enge Begriff der Verlustfunktion betrachtet.

Die Verlustfunktionen (*LossFunction*) im Rahmen dieser Arbeit basieren auf Störungen in den Anwendungssystemen, die über den Betrieb (*operate*) der zentralen Aktivitäten (*Activity*) die Wertkette beeinflussen.

$$LossFunction \equiv Activity \; \forall \; operate.Asset \tag{4.21}$$

Die Störungen der Assets werden dabei entsprechend der eingeführten Supportfunktion (vgl. Formel 4.12) modelliert. Die Höhe der finanziellen Verluste leitet sich nun aus den mit der Aktivität verbundenen (*generate*) Effekten ab. Diese stellen hier unternehmenskritische Größen (z.B. Tagesrenditen, Handels- oder Abwicklungsvolumen) dar, die durch eine Störung der Anwendungssysteme negativ verändert werden. Die Modellierung der Verluste erfolgt unabhängig von den auslösenden Ereignissen (vgl. Kühn und Neu 2004, S.6). Entsprechend dem allgemeinen Simulationsmodell werden die finanziellen Verluste hier als Ausgabegrößen (*Output*) in das Modell integriert.

$$Output \equiv Loss \ \forall\, generate.LossFunction \tag{4.22}$$

Die entstehenden Verluste sind nicht konstant. Sie ermitteln sich aus den vom Ausfall betroffenen Geschäften in der Wertschöpfung (z.B. Handelsgeschäfte oder Kredite). Im Rahmen des Ontologie-zentrierten Simulationsmodells wird der Verlust einer Aktivität der Wertkette als eine stochastische Zufallsgröße interpretiert (vgl. Leippold und Vanini 2003, S.10; Kühn und Neu 2004, S.6). In deren Ermittlung gehen Annahmen über die Verteilung der kritischen Größen einer Aktivität sowie über die abzuleitenden finanziellen Verluste ein. Um die Berechnung in das Modell zu integrieren, wird wiederum das Konstrukt der *formula* erweitert.

$$\geqslant 1\ (\ formula.String\ ) \sqsubseteq Output \tag{4.23}$$

Die Verlusthöhe wird hier durch zwei Einflussgrößen bestimmt. Einerseits differiert die Verlusthöhe in Abhängigkeit vom Anwendungssystem und der hiervon betroffenen Aktivität der Wertkette (vgl. Leippold und Vanini 2003, S.10). Andererseits sind Volumen und Art der betroffenen Geschäfte relevant für die Höhe des finanziellen Effekts (vgl. Spahr 2001, S.661).

Der Verlust L_O aus einem *Output O* folgt einer stetigen, unabhängigen Zufallsvariablen *X* mit festgelegter Verteilung, die die Höhe in Abhängigkeit von Einflussgrößen, wie dem Abwicklungsvolumen oder der täglichen Rendite, modelliert. Die Abschätzung der Verteilungsparameter wiederum muss die relevanten Einflussgrößen reflektieren.

Für die Modellierung der Verlusthöhe kann eine Vielzahl an Verteilungen verwendet werden (vgl. Cruz 2002, S.39ff.) Als gängige Verteilungen werden die Normal-, die Lognormal-, die Weibull- sowie die Gamma -Verteilung vorgestellt. Davon werden besonders die Lognormal- und die Weibull-Verteilung aktuell bei Banken eingesetzt (vgl. Deutsche Bundesbank und BaFin 2005, S.18). Zur Veranschaulichung werden nachfolgend jeweils die Dichtefunktion sowie die ersten beiden Momente eingeführt.

Die Normalverteilung ist eine wichtige Verteilung im Bereich der Finanzmarkttheorie, deren besondere Bedeutung aus dem zentralen Grenzwertsatz resultiert (vgl. Hesse 2003, S. 179). Folgend ist die Dichtefunktion der Normalverteilung mit Mittelwert μ und Standardabweichung σ dargestellt:

$$f_{(\mu,\sigma)}(z) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-(z-\mu)^2/2\sigma^2} \quad \forall z \in \mathbb{R} \tag{4.24}$$

Da im Bereich operationeller Risiken verstärkt Verluste im extremen Randbereich von Bedeutung sind (vgl. Kapitel 4.2.2.c), ist die Normalverteilung für das hier entwickelte Modell nur eingeschränkt geeignet. *„[...] the events in operational risk will hardly ever follow a Gaussian pattern.“* (Cruz 2002, S.50)

Die ersten beiden Momente entsprechen den Parametern der Verteilung:

$$E(X) = \mu \quad \text{und} \quad V(X) = \sigma^2 \tag{4.25}$$

Die Lognormal-Verteilung wird insbesondere im Bereich der Versicherungen zur Schätzung der Schadenhöhe verwendet. Aufgrund der im Vergleich zur Normalverteilung stärker ausgeprägten Ränder, kommt diese Verteilung auch bei Banken zur Modellierung operationeller Risiken zum Einsatz. Ihre Dichtefunktion stellt sich wie folgt dar:

$$f_{(\mu,\sigma)}(z) = \frac{1}{\sqrt{2\pi\sigma^2}} \frac{1}{z} e^{-(\ln z-\mu)^2/2\sigma^2} \quad \forall z \in \mathbb{R}^+ \tag{4.26}$$

Die ersten beiden Momente ergeben sich als (vgl. Beyer et al. 1980, S.79):

$$E(X) = e^{\mu+\sigma^2/2} \quad \text{und} \quad V(X) = e^{2\mu+\sigma^2}(e^{\sigma^2}-1) \tag{4.27}$$

Die Weibull-Verteilung stellt eine verallgemeinerte Form der Exponential-Verteilung dar (vgl. Nowack 1994, S.62). Sie wird häufig zur Modellierung von Lebensdauern in der Qualitätssicherung eingesetzt. Insbesondere die Zuverlässigkeitsmodelle im Bereich von Hardware (vgl. Musa, Iannino und Okumoto 1987, S.251) greifen häufig auf diese Verteilung zurück. Ferner spielt die Weibull-Verteilung im Rahmen der Extremwerttheorie als Verteilung mit „medium tail“ (vgl. Moscadelli 2004, S.69) eine entscheidende Rolle:

$$f_{(\tau,\eta)}(z) = \frac{\eta}{\tau}\left(\frac{z}{\tau}\right)^{\eta-1} e^{-(z/\tau)^\eta} \quad \forall z \in \mathbb{R}^+,\ \eta>0,\ \tau>0 \tag{4.28}$$

Der Erwartungswert und die Varianz der Weibull-Verteilung ergeben sich wie folgt (vgl. Beyer et al. 1980, S.79):

$$E(X) = \tau\, \Gamma(1+\frac{1}{\eta}) \quad \text{und} \quad V(X) = \tau^2 (\Gamma(1+\frac{2}{\eta}) - (\Gamma(1+\frac{1}{\eta})^2)) \tag{4.29}$$

Abschließend wird die Gamma-Verteilung vorgestellt. Auch diese Verteilung findet im Bereich der Zuverlässigkeitsanalyse von Software Verwendung (vgl. Pham 2000, S.28). Die Dichtefunktion der Gamma-Verteilung wird wie folgt definiert (vgl. Hesse 2003, S.162):

$$f_{(\lambda,r)}(z) = \frac{\lambda^r}{\Gamma(r)} z^{r-1} e^{-\lambda z} \qquad \forall z \in \mathbb{R}^+,\ r \in \mathbb{N},\ \lambda > 0 \tag{4.30}$$

Eine besondere Eigenschaft der Gamma-Verteilung ist ihre Reproduktivität. Die ersten beiden Momente ergeben sich wie folgt (vgl. Hesse 2003, S.162):

$$E(X) = \frac{r}{\lambda} \qquad \text{und} \qquad V(X) = \frac{r}{\lambda^2} \tag{4.31}$$

Die folgende Abbildung 4.1 zeigt die Dichtefunktionen der oben eingeführten Verteilungen. Um die Vergleichbarkeit zu gewährleisten, sind die jeweiligen Lageparameter so gewählt, dass in allen Fällen der Erwartungswert 100 Mio. EUR und die Standardabweichung 50 Mio. EUR entspricht. Der $VaR_{99,9}$ zeigt in Abhängigkeit von der betrachteten Verteilung deutliche Unterschiede.

4.3.5 Simulation des stochastischen Verlustprozesses

Die Ermittlung des gesamten Verlustpotentials aus Technologierisiken erfolgt über die Definition eines stochastischen Verlustprozesses. Als Zeiteinheit hierfür wird ein (Handels-)Tag gewählt (vgl. Kühn und Neu 2003, S.656; Leippold und Vanini 2003, S.20). Für jeden Tag ergeben die Werte der Zustände sämtlicher Risikofaktoren, in Verbindung mit den definierten Abhängigkeiten, die Zustandswerte der Assets. Hieraus leitet sich wiederum ab, ob ein bestimmter Verlust eintritt oder nicht.

Um das Verlustpotential zu berechnen, wird der Betrachtungszeitraum auf 365 aufeinander folgende Tage festgelegt (vgl. Basel II, Tz.667) und die in diesem Zeitraum eingetretenen Verluste addiert. Der potentielle Verlust über ein Jahr entspricht also der Summe aller Einzelverluste über die Tage.

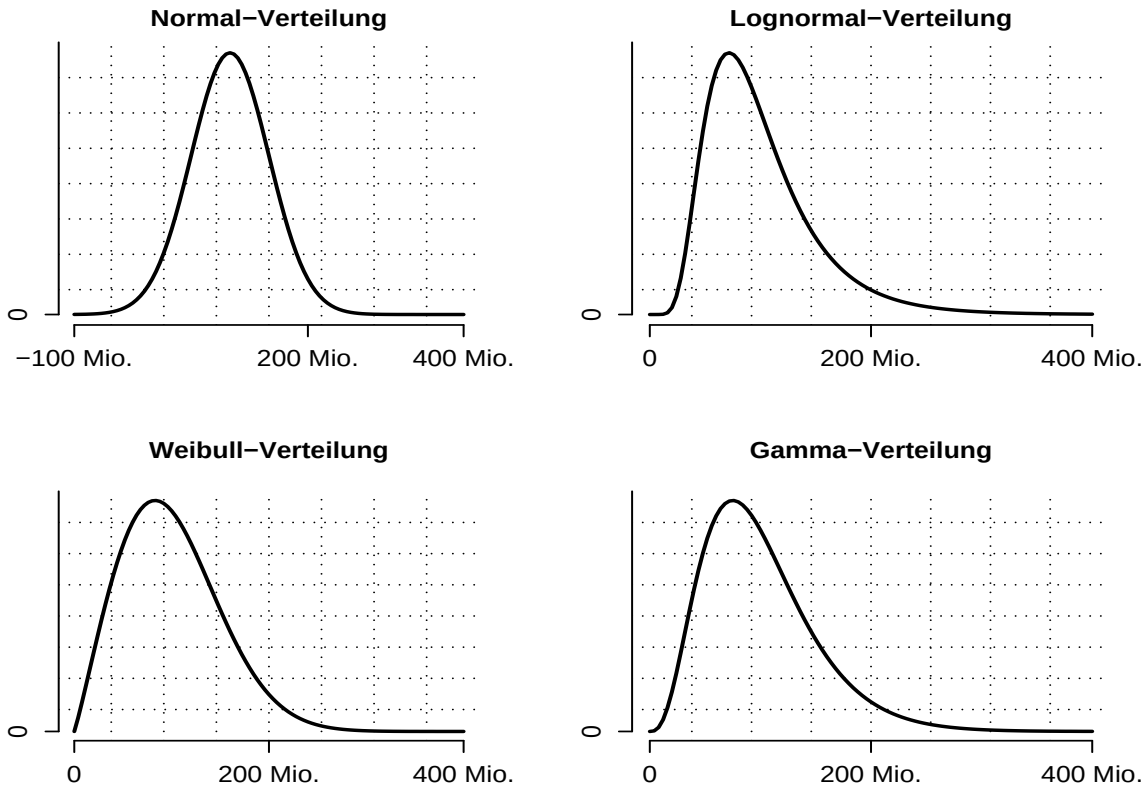

Abbildung 4.1: Mögliche Verteilungen mit unterschiedlichen Rändern

Normalverteilung μ = 100.000.000 und σ = 50.000.000, mit $VaR_{99,9}$ = 254.511.615
Lognormal-Verteilung μ = 18,31 und σ = 0,47, mit $VaR_{99,9}$ = 385.066.168
Weibull-Verteilung τ = 112.910.000 und η = 2,10, mit $VaR_{99,9}$ = 283.237.262
Gamma-Verteilung λ = 0.00000004 und r = 4, mit $VaR_{99,9}$ =326.556.020

Der Betrachtungszeitraum von einem Jahr entspricht der aufsichtsrechtlichen Sichtweise (vgl. Haubenstock und Hardin 2003, S.172). Der stochastische Verlustprozess wird formal als Summe der Verluste L_o über 365 Tagen definiert:

$$L(T) = \sum_{t=1}^{T} \sum_{O=1}^{\|Output\|} L_O(t) \tag{4.32}$$

Die Ermittlung der Verteilungsfunktion des Gesamtverlustes *L(T)* kann entweder analytisch oder mittels einer Simulation erfolgen. Für eine analytische Lösung stehen theoretisch unterschiedliche Ansätze zur Verfügung (vgl. Frachot, Georges und Roncalli 2001, S.5f.; Embrechts, Furrer und Kaufmann 2003, S.6f.): Näherungsverfahren, Inversionsmethode oder Rekursion. Für eine detaillierte Darstellung der unterschiedlichen Möglichkeiten sei auf die Literatur und die dort angegebenen Quellen verwiesen.

Im Bereich der Technologierisiken gibt es vielmals keine analytische Lösung zur Ermittlung der Gesamtverlustverteilung (vgl. Kühn und Neu 2004, S.7). Daher wird in dieser Arbeit hierzu eine Simulation eingesetzt. Zunächst werden die Eingabewerte für das Modell (*Input*) über die angenommene Wahrscheinlichkeitsverteilung für die Risikofaktoren berechnet. Im nächsten Schritt werden die Zustände der Modellelemente (*Element*) über die beeinflussenden Risikofaktoren und über die zwischen den Anwendungssystemen definierten Abhängigkeiten (Formeln 4.12 und 4.13) ermittelt. Die Einzelverluste (*Output*) werden über die jeweilige Verlustverteilung bestimmt. Das gesamte Verlustpotential wird als Summe der Einzelverluste (Formel 4.32) über den Betrachtungszeitraum ermittelt. Dieser Vorgang wird entsprechend der Anzahl Simulationsschritte wiederholt. Die Approximation einer Wahrscheinlichkeitsverteilung aus den simulierten Daten erfolgt über die Schätzung einer Kernel-Dichte. Zur Messung des Risikopotentials werden die in den Grundlagen (vgl. Kapitel 2.1.3) dargestellten Risikomaße VaR und CVaR verwendet. Die Vorgehensweise ist im folgenden Pseudocode schematisch zusammengefasst:

```
Für Iteration i in {1..Anzahl Iterationen}
    Für Tag t in {1..365}
        Input[] = Ermittle_Input()
        Element[] = Ermittle_Element(Input[])
        Output[] = Ermittle_Output(Element[])
        Verlust[i] += Summe(Output[])
Berechne_VaR (Verlust[])
Berechne_CVaR (Verlust[])
```

Die Qualität der Simulation ist abhängig von der Anzahl Simulationsschritte. So kann die Genauigkeit des Modells mit steigender Anzahl Iterationen erhöht werden, wodurch jedoch die Laufzeit steigt. Ein häufig verwendetes Kriterium für eine Abschätzung der erforderlich Anzahl ist die Konvergenz der simulierten Ergebnisse (vgl. Frachot, Georges und Roncalli 2001, S.7ff.). Die konkrete Anzahl benötigter Iterationen hängt im Einzelfall jedoch wesentlich von der Komplexität des jeweiligen Graphen sowie dem verwendeten Risikomaß ab.

4.3.6 Überblick und kritischer Vergleich

Die Vorgehensweise der Ontologie-zentrierten Simulation besteht im Kern aus der zweistufigen Transformation der Technologierisiko-Ontologie (vgl. Abbildung 4.2). Grundlage ist das auf einer formalen Ontologie basierende Technologierisiko-Modell (*ITComponent, ITManagementTask, ApplicationSystem, Property, Activity, Loss*).

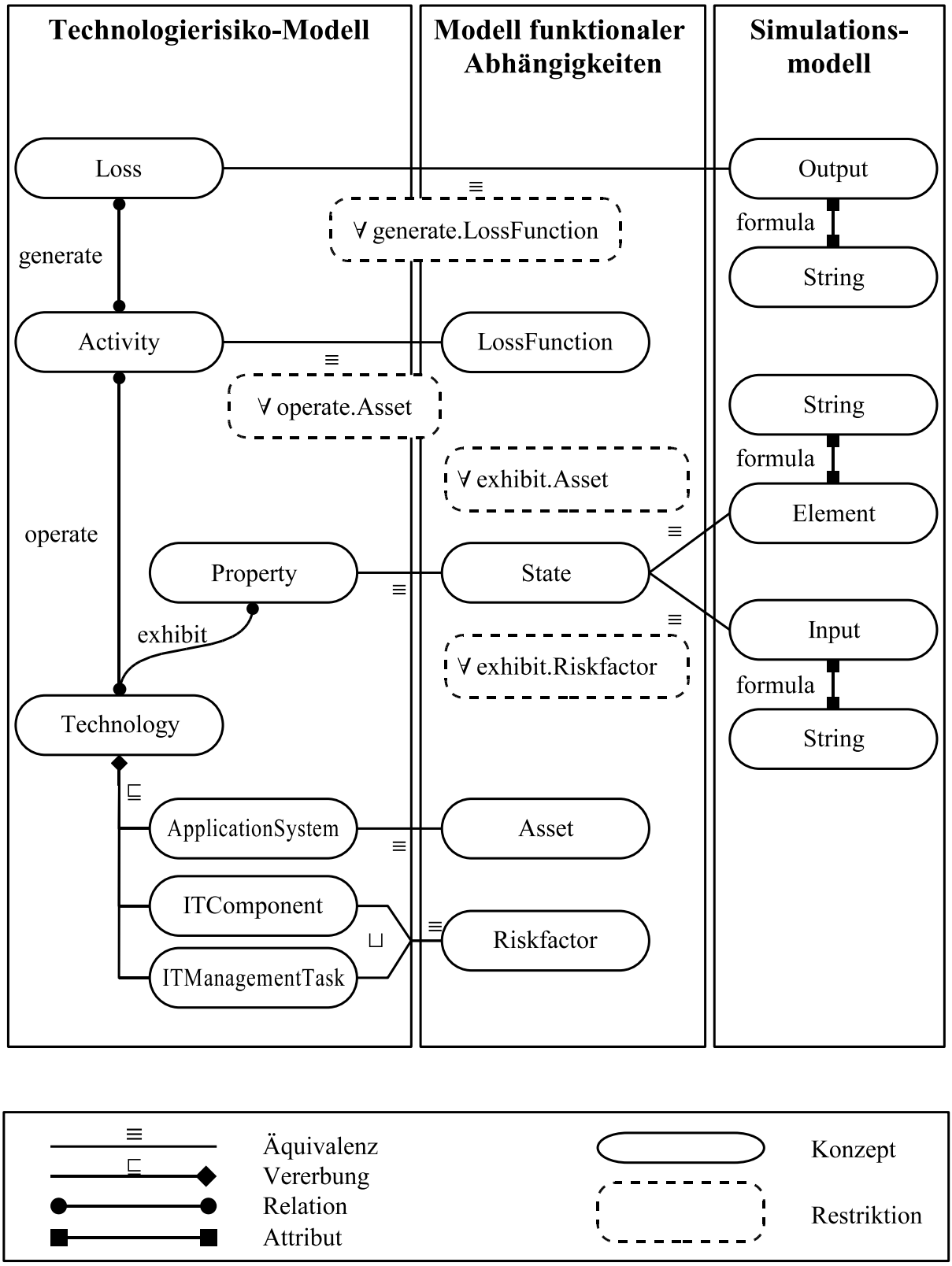

Abbildung 4.2: Überblick Ontologie-zentrierte Simulation

Die erste Stufe der Transformation legt die allgemeine Überführung des Technologierisiko-Modells in ein Modell auf Basis funktionaler Abhängigkeiten (*Riskfactor, Asset, State, LossFunction*) fest. Hieraus wird dann in einem zweiten Transformationsschritt das Simulationsmodell (*Input, Element, Output*) abgeleitet. Sämtliche Annahmen über die Berechnungen der Simulation, wie beispielsweise die jeweiligen Verteilungen, sind ausschließlich in dem Attribut *formula* enthalten.

Die folgende Tabelle 4.7 zeigt die charakteristischen Merkmale der Ontologie-zentrierten Simulation. Der Aufbau entspricht dabei dem Vergleich der unterschiedlichen Ansätze zur Modellierung funktionaler Abhängigkeiten (vgl. Tabelle 4.5).

Komponenten	Umsetzung
Elemente	**Für die Wertkette relevante Anwendungssysteme**
Wertebereiche der Zustände	Diskret {0,1}, Step-Funktion
Betrachtetes Zeitintervall	Δt
Zeitabhängigkeit	Bezug zu t-$\alpha\Delta t$
Regeneration	In Δt
Risikofaktoren	**IT-Komponenten und IT-Managementaufgaben**
Betrachtete Zustände	Unabhängig Bernoulli-verteilt, {0,1}
Störgröße	Standardnormal-verteilt
Verlustfunktion	**Finanzielle Verluste**
Wertebereich	Stetig, z.B. Lognormal-, Weibull oder Gamma-Verteilung
Verknüpfung	Unabhängige Zufallsvariable
Ermittlung der Verlustverteilung	**Simulation**
Zeitintervall	Δt = 1 Tag
Zeitraum	1 Jahr = 365 Tage

Tabelle 4.7: Merkmale der Ontologie-zentrierten Simulation

Der vollständige Ablauf einer Quantifizierung operationeller Technologierisiken mittels der Vorgehensweise der Ontologie-zentrierter Simulation entspricht folgendem schematischen Aufbau:

1. Beschreibung der Risikosituation auf Basis der Konzepte des Technologierisiko-Modells:
   - *ITComponent*
   - *ApplicationSystem*
   - *ITManagementTask*
2. Zweistufige Transformation in ein Simulationsmodell bestehend aus:
   - *Input*
   - *Element*
   - *Output*
3. Schätzung der Simulationsparameter:
   - Wahrscheinlichkeit p der Bernoulli-Verteilung der Risikoereignisse
   - Ausgangssupportwert ϑ, Gewichte ω, β und ξ sowie Zeitabhängigkeit α
   - Verteilung sämtlicher Einzelverluste und deren Parameter
4. Durchführung der Simulation (vgl. Kapitel 4.3.5).

Eines der zentralen Probleme simulationsgestützter Vorgehensweisen ist die Schätzung der Parameter. Im vorgeschlagenen Modell werden daher an zwei Stellen vereinfachende Annahmen getroffen: Zum einen folgen die Risikofaktoren einer diskreten Bernoulli-Verteilung, zum anderen wird eine vollständige Regeneration der Zustände innerhalb von Δt unterstellt. Als Ergänzung wird eine mehrstufige Zeitabhängigkeit vorgesehen, die einen Bezug zu beliebigen vorangegangenen Zeitpunkten (Tagen) ermöglicht. Durch die Trennung der Formeln zur Berechnung der Support- und Verlustfunktionen von den strukturellen Zusammenhängen im Modell, kann eine Erweiterung im Hinblick auf die Regeneration und Stetigkeit jederzeit erfolgen. Durch die automatische Transformation der auf Basis der Technologierisiko-Ontologie entwickelten Modelle in die Simulationsmodelle kann ferner die semantische Lücke zwischen fachlicher und technischer Sicht verringert werden. So trägt die Ontologie-zentrierte Vorgehensweise dazu bei, dieses wesentliche Problem der Entwicklung von Simulationsmodellen zu reduzieren.

4.4 Zusammenfassung

Das zweite zentrale Ziel dieser Arbeit ist die Entwicklung einer wissensbasierten Methode zur Quantifizierung operationeller Technologierisiken. Das impliziert, dass die Methode nicht nur den allgemeinen quantitativen Anforderungen gerecht wird, sondern auch das Risikoverständnis im Sinne der in Kapitel 3 entwickelten Ontologie als zentralen Baustein enthält. In Kapitel 4.2.4 wurden die wesentlichen existierenden Methoden und Modelle im Hinblick auf die beiden

Zieldimensionen einander gegenübergestellt (vgl. Tabelle 4.6). Die vorgeschlagene Methode der Ontologie-zentrierten Simulation stellt in diesem Sinne sicherlich einen weiteren Fortschritt dar, da die Vorteile des Modells funktionaler Abhängigkeiten unmittelbar mit einem expliziten Verständnis operationeller Technologierisiken verknüpft werden. Die Abbildung 4.3 fasst die Vorteilhaftigkeit des in Kapitel 4.3 vorgeschlagenen Methode im Hinblick auf die beiden Dimensionen Verständnis und Quantifizierung noch einmal zusammen.

Entscheidend für die Bewertung der Methode sind darüber hinaus jedoch auch finanzielle Kriterien, wie die Auswirkung auf das regulatorische Kapital oder entstehende Kosten. Denn zwangsläufig müssen Banken unterschiedliche Modelle auch nach der Höhe der ermittelten Eigenkapitalunterlegung beurteilen (siehe Fitch 2004). Ferner spielen zusätzlich die Kosten bei der Implementierung des Modells eine wichtige Rolle.

Es ist davon auszugehen, dass die höhere Komplexität zumindest zusätzliche Kosten verursacht. Eine Auswirkung auf die Eigenkapitalunterlegung kann ex ante jedoch nicht prognostiziert werden. Im Allgemeinen wird davon ausgegangen, dass eine Betrachtung der Korrelationen oder Zusammenhänge eher zu einer Reduktion führt (siehe Fitch 2004). Insofern ist mit wachsender Zielerreichung (vgl. Abbildung 4.3) einerseits mit steigenden Einführungskosten zu rechnen. Die Höhe des regulatorischen Eigenkapitals wird andererseits im Einzelfall zu untersuchen sein.

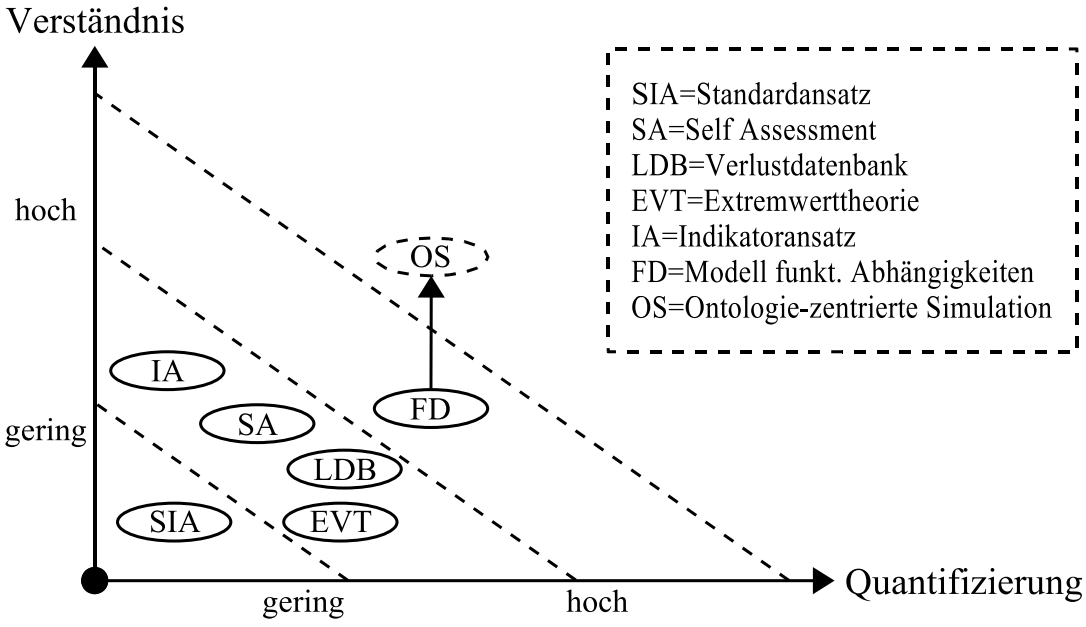

Abbildung 4.3: Zielerreichung der Methoden

Die vorgeschlagene Methode wird in einem weiteren Schritt daraufhin untersucht, in welchem Umfang die Anforderungen aus Basel II umgesetzt werden können. Ein vollständiger Abgleich sämtlicher Kriterien ist hier nicht Gegenstand der Betrachtung, da dies wesentlich von der konkreten Umsetzung innerhalb des betrachteten Kreditinstitutes abhängt. Vielmehr soll die Integrierbarkeit in den fortgeschrittenen Messansatz anhand der zentralen qualitativen und quantitativen Anforderungen untersucht werden (siehe Basel II):

Kriterium	Entsprechung
Tz.667 Berücksichtigung extremer Verluste	Eine Erweiterung der Simulationsergebnisse über die Extremwerttheorie ist jederzeit möglich.
Tz.669.(a) Entsprechung Risikodefinition	Das in der Technologierisiko-Ontologie enthaltene Verständnis ist konform mit Basel II.
Tz.669.(d) Berücksichtigung von Korrelationen	Funktionale Abhängigkeiten sind ein Bestandteil des Modells, stochastische Korrelationen sind möglich.
Tz.670, Tz.671 Sammlung interner Verlustdaten	Die Technologierisiko-Ontologie kann verwendet werden, verschiedene Schemata zu verbinden.
Tz.674 Sammlung externer Verlustdaten	Die Technologierisiko-Ontologie kann verwendet werden, verschiedene Schemata zu verbinden.
Tz.675 Szenarioanalysen / Expertenwissen	Die Technologierisiko-Ontologie kann genutzt werden, um z.B. Fragebögen zu generieren.
Tz.676 Einflussfaktoren	Mögliche Risikoindikatoren können in die Ontologie integriert werden.

Tabelle 4.8: Integrierbarkeit in fortgeschrittenen Messansatz

Als Fazit kann festgehalten werden, dass die vorgeschlagene Methode effizient in einen fortgeschrittenen Messansatz integriert werden kann. Das in der Technologierisiko-Ontologie vorgesehene Mapping (vgl. Abbildung 3.3) kann dazu genutzt werden, das Problem der Überleitung individueller Verlustdatenschemata in das aus Geschäftsfeldern und Ereignistypen bestehende Modell von Basel II (vgl. Schäl und Stummer 2005, S.786) zu reduzieren.

Da die Quantifizierung wiederum nur einen Teil des gesamten Risikomanagementprozesses ausmacht, muss eine Integration des vorgeschlagenen Modells in den gesamten Prozess möglich sein. Hierzu ist es notwendig, die Ontologie mit den Methoden der anderen Phasen des Risikomanagementprozesses zu kombi-

nieren. Für die Phase der Identifikation beispielsweise kann die unternehmensweite Ontologie in ein Modell transformiert werden, das zur Erzeugung von Fragebögen oder zur Strukturierung der gewonnenen Informationen benutzt wird. So können Techniken des Wissensmanagements helfen, die Identifikation von Risiken zu unterstützten. Ebenso können für die Phase der Steuerung mögliche Kontrollen in ein transformiertes Modell eingebettet werden, um deren Wirksamkeit zu simulieren. Ferner kann das automatische Reasoning verwendet werden, um die Entscheidungsfindung in der IT-Governance zu unterstützen.

Ontologien können auch zur Interaktion und Integration von Software verwendet werden (vgl. Kapitel 2.3.1). Daher kann in einer technischen Umsetzung der Einbettung in den Risikomanagementprozess oder der Transformation in das Simulationsmodell wiederum auf Eigenschaften formaler Ontologien zurückgegriffen werden.

Um die prototypische Implementierung der im Rahmen dieser Arbeit entwickelte Methode der Ontologie-zentrierten Quantifizierung zu beschreiben, werden im folgenden Kapitel die relevanten technischen Details vorgestellt.

Kapitel 5
Implementierung

Um die technische Machbarkeit eines modelltheoretischen Konzeptes zu demonstrieren, wird häufig die Alternative der Entwicklung eines Prototyps gewählt. In diesem Sinne wird die in den Kapiteln 3 und 4 vorgeschlagene Vorgehensweise zur Risikoquantifizierung im Folgenden prototypisch umgesetzt. So können die entscheidenden Aspekte der Implementierung evaluiert und ein technischer „proof of concept“ geliefert werden. Ebenso ist eine technische Realisierung der Ontologie-zentrierten Simulation erforderlich, um für das in Kapitel 6 vorgestellte Fallbeispiel die Risikoquantifizierung unterschiedlicher Szenarien vornehmen zu können.

Bei der Implementierung steht die Technologierisiko-Ontologie im Mittelpunkt. Daher trägt die Anwendung deutliche Züge eines Wissensmanagementsystems. Dieser Begriff umfasst allgemein *„[...] a class of information systems applied to managing organizational knowledge. That is they are IT-based systems developed to support and enhance the organizational knowledge process of knowledge creation, storage/retrieval, transfer and application“* (Alavi und Leidner 2001, S.114). In den folgenden Abschnitten wird, aufbauend auf der allgemeinen Architektur des Prototyps, die Umsetzung der grundlegenden Technologierisiko-Ontologie in der OWL (creation), die Verarbeitung des jeweiligen Bankmodells (storage/retrieval) sowie die Transformation in ein Simulationsmodell über Ontology Views (transfer) beschrieben. Abschließend wird die Erzeugung des Java-basierten Simulationscodes und die mittels R-Skripten realisierte Auswertung (application) dargestellt.

5.1 Architektur

Die prototypische Anwendung zur Umsetzung der Risikoquantifizierung wird auf Basis der Technologierisiko-Ontologie konzipiert, um entsprechend Definition 2.4 diese auch in das Zentrum der technischen Realisation zu stellen. Das Wissensmodell steht somit im Mittelpunkt der Architektur, die einzelnen Be-

standteile der Anwendung werden sukzessive hiermit verbunden. Hierdurch ist jedoch die Anwendung in hohem Maße abhängig von den Konzepten und Relationen der Technologierisiko-Ontologie. Da das beschriebene Modell operationeller Technologierisiken nicht als abgeschlossen angesehen werden kann (vgl. Kapitel 3.3), ist eine möglichst lose Kopplung des Programms und der Ontologie wünschenswert. So kann auf mögliche Änderungen an der Ontologie flexibel reagiert werden. An wenigen Stellen machen jedoch programmspezifische Besonderheiten eine Abbildung der Konzepte im Java Code notwendig. Auf diese Limitation wird an der entsprechenden Stelle jeweils explizit hingewiesen.

Der entwickelte Prototyp ist im Kern in Java implementiert. Die graphische und numerische Analyse erfolgt mittels R-Skripten (siehe R Development Core Team 2005). Ergänzend kommen externe Java-Bibliotheken und R-Pakete zum Einsatz. Die grundlegende Architektur der Anwendung ist in Abbildung 5.1 schematisch dargestellt. Im Folgenden wird zunächst ein Überblick der zentralen internen und externen Komponenten ❶ bis ❼ gegebenen.

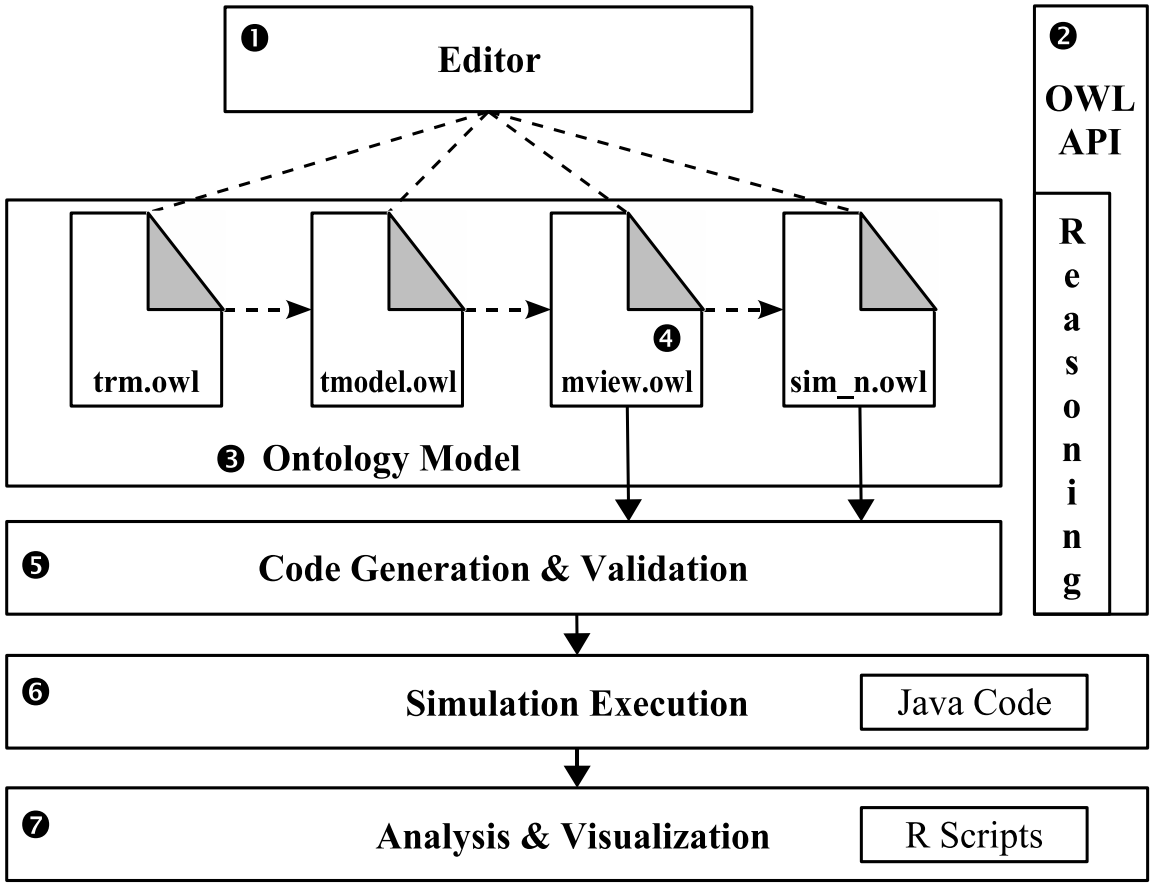

Abbildung 5.1: Architektur des Prototyps

Die Bearbeitung der gesamten Ontologie erfolgt mittels eines geeigneten Editors (❶). Hierfür kommen entweder reine Ontologie-Editoren, wie beispielsweise Protégé (siehe Stanford Medical Informatics 2005), oder graphische, an die Domäne individuell angepasste Benutzeroberflächen in Frage. Da es sich bei der hier vorgestellten Anwendung um einen Prototyp handelt, wird auf eine graphische Komponente verzichtet und die Bearbeitung der Ontologien ausschließlich über den OWL-Editor Protégé vorgenommen.

Für die Verarbeitung der Ontologien (❷) innerhalb der Anwendung, wie das Parsen der OWL-Dateien, die Durchführung des Reasonings oder das Speichern der Ontologie, wird auf ein standardisiertes OWL-API zurückgegriffen. Hier kommt die Java-basierte Bibliothek Jena (HP Labs Semantic Web Research 2005) zum Einsatz.

Das Ontologie-Modell (❸) besteht im Detail aus verschiedenen OWL-Dateien. Diese enthalten die unterschiedlichen Aspekte der vorgeschlagenen Methode zur Quantifizierung von Technologierisiken. Die Dateien bauen dabei direkt aufeinander auf. Strukturen (Konzepte, Relationen, Restriktionen) und Individuen werden grundsätzlich separiert. Der Inhalt der einzelnen Dateien stellt sich wie folgt dar:

- Die in Kapitel 3 vorgestellte Technologierisiko-Ontologie stellt die Grundlage des Ontologie-Modells dar. In der zugehörigen Datei `trm.owl` sind sämtliche Konzepte, Relationen und Restriktionen des Modells operationeller Technologierisiken enthalten.
- In der Datei `tmodel.owl` wird die konkrete Ausprägung des Modells für ein Kreditinstitut basierend auf den in `trm.owl` beschriebenen Strukturen dargestellt. Die Datei enthält ausschließlich Individuen.
- Die Regeln für die Transformation (❹) des auf der Technologierisiko-Ontologie `trm.owl` beruhenden bankspezifischen Modells `tmodel.owl` in das in Kapitel 4.3 beschriebene Simulationsmodell werden in der Datei `mview.owl` spezifiziert.
- Die Dateien `sim_n.owl` stellen jeweils ein konkretes Simulationsmodell für ein Szenario *n* dar. Es basiert auf der Transformation `mview.owl` Hierin sind die für die Simulation relevanten Verteilungsparameter und Formeln enthalten. Die in Kapitel 6.3 erstellten Szenarien sind als solche Dateien gespeichert.

Die Überführung des Simulationsmodells in ein ausführbares Java Programm (❺) wird mittels einer Template-basierten Quellcode-Generierung realisiert. Der erzeugte Code wird dabei als Methode einer Simulationsklasse kompiliert.

Die für die Simulation erzeugte Klasse wird dynamisch über einen Class-Loader geladen und instantiiert und dann die Methode zur Simulation ausgeführt (❻). Für die Generierung der während der Simulation benötigten Zufallszahlen wird die Java-basierte Bibliothek SSJ (siehe L'Ecuyer 2001) verwendet.

Die graphische und numerische Analyse der Simulationsergebnisse (❼) wird mit Hilfe von R-Skripten durchgeführt (siehe R Development Core Team 2005). Die automatische Verbindung von Java mit R erfolgt hierbei über das Java Native Interface (JNI) (siehe RoSuDa 2005).

In den folgenden Kapiteln werden die wichtigsten Aspekte der technischen Umsetzung der Ontologie in OWL (❷-❸), der Transformation der Ontologie in das Simulationsmodell (❹) und der Erzeugung, Durchführung und Auswertung der Simulation (❺-❼) detailliert aufgegriffen.

5.2 Umsetzung der Ontologie in OWL

Grundlage der Implementierung formaler Ontologien sind die auf First Order Logic oder Frames basierenden Sprachen zur Repräsentation von Wissen, wie KIF, LOOM oder Flogic. Für eine detaillierte Übersicht wird auf die Literatur verwiesen (vgl. Gomez-Perez, Fernandez-Lopez und Corcho 2004, S.199ff.). Eine wichtige Weiterentwicklung dieser Sprachen zur Implementierung von Ontologien resultiert aus der Idee des Semantic Web:

„[It] is not a separate Web but an extension of the current one, in which information is given well-defined meaning, better enabling computers and people to work in cooperation.“ (Berners-Lee, Hendler und Lassila 2001, S.35)

In diesem Kontext wurden gezielt Sprachen zur semantischen Anreicherung von Internetinhalten entwickelt. Darunter fallen beispielsweise das Resource Description Framework (RDF) (siehe W3C 2004c), RDF Schema (RDFS) (siehe W3C 2004b) und auch die Web Ontology Language (OWL) (siehe W3C 2004a). Abbildung 5.2 zeigt den zusammenhängenden Aufbau dieser Sprachen. Grundlage stellt die Syntax der Extensible Markup Language (XML) basierend auf Uniform Resource Identifier (URI) und Unicode dar. Aufbauend darauf wurde RDF zur Beschreibung von Internetseiten mit Meta-Daten entwickelt. Hierüber können beliebigen Ressourcen relevante Eigenschaften oder Werte zugeordnet werden. Darüber hinaus ermöglicht RDFS, die in RDF verwendeten Ressourcen, Eigenschaften und Werte über die Bildung von Klassen oder die Einschränkung zulässiger Eigenschaften genauer zu beschreiben. So kann mittels RDFS den Ausdrücken in RDF eine klare Semantik gegeben werden (vgl. McBride 2004, S.51f).

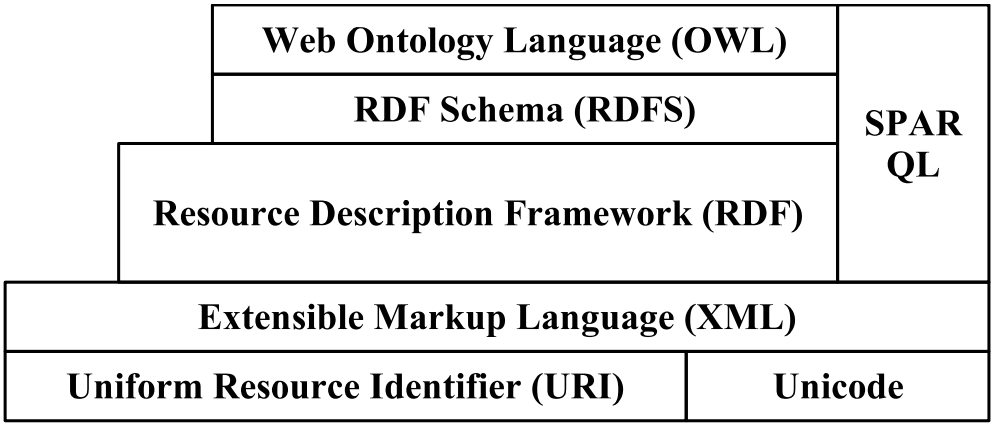

Abbildung 5.2: Hintergrund OWL
(siehe Berners-Lee, Hendler und Lassila 2001)

Mit der Anfragesprache SPARQL (siehe W3C 2006) existiert seit 2006 zudem eine standardisierte Möglichkeit, Anfragen an RDF- oder auch OWL-Dokumente zu stellen.

Mit dem aktuellen Entwurf für die OWL (2004) hat das World Wide Web Consortium (W3C) andere XML-basierte Implementierungssprachen wie zum Beispiel DAML oder OIL zu einem gemeinsamen, auf RDF(S) basierenden Standard zusammengeführt. Ziel der Entwicklung war die Schaffung eines akzeptierten Standards mit einer im Vergleich zu RDF(S) erweiterten Ausdrucksstärke (vgl. Antoniou und Van Harmelen 2004, S.67). Mit der OWL wurden damit die entscheidenden existierenden Ansätze zur XML-basierten Implementierung von Ontologien aufgegriffen. Da die OWL somit einen Quasi-Standard darstellt, wird sie im Rahmen dieser Arbeit zur Umsetzung der Technologierisiko-Ontologie eingesetzt.

Bei der Entwicklung von OWL mussten insbesondere zwei Anforderungen berücksichtigt werden. Es sollte eine vollständige Abwärtskompatibilität mit RDFS gegeben sein und dabei gleichzeitig ein effizientes Reasoning ermöglicht werden. Hieraus ergibt sich jedoch aufgrund des Sprachumfangs von RDFS ein Widerspruch (vgl. Antoniou und Van Harmelen 2004, S.70). Um diesem Sachverhalt Rechnung zu tragen, wurde die OWL in drei möglichen Ausprägungen vorgeschlagen:

- OWL-Full ist vollständig kompatibel zu RDFS. Jedoch ist das Reasoning nicht entscheidbar, da die verwendeten Algorithmen nicht zwangsläufig in endlicher Zeit terminieren.

- OWL-DL garantiert entscheidbares Reasoning, also die effiziente Berechenbarkeit, da es sich direkt in DL (konkret $\mathcal{SHOIN}$) überführen lässt. Die wesentliche Einschränkung gegenüber OWL-Full ist, dass jedes Artefakt nur entweder Konzept, Relation oder Individuum sein kann.
- OWL-Lite stellt eine eingeschränkte Version von OWL-DL dar, mit dem Ziel, eine einfache Entwicklung von OWL-Tools zu unterstützen. Verglichen mit OWL-DL sind insbesondere die Möglichkeiten, Konzepte zu beschreiben, eingeschränkt.

Für die Entwicklung des Prototyps wird OWL-DL verwendet, um die maximale Ausdrucksstärke bei effizientem Reasoning zu erreichen. Um die in Kapitel 3.2 formalisierte Technologierisiko-Ontologie und die in Kapitel 4.3 definierte Transformation implementieren zu können, wird in Tabelle 5.1 die in dieser Arbeit verwendete DL (vgl. Tabelle 2.3) auf korrespondierende Ausdrücke in OWL-DL abgebildet.

DL	**OWL-DL**	**Abstract Syntax**
$\top$	<owl:Thing>	owl:Thing
C	<owl:Class rdf:ID="C">	Class(C)
$C_1 \equiv C_2$	<owl:equivalentClass rdf:resource="C₂">	EquivalentClasses(C₁ C₂)
$C_1 \sqsubseteq \neg C_2$	<owl:disjointWith rdf:resource="C₂">	DisjointClasses(C₁ C₂)
$C_1 \sqsubseteq C_2$	<rdfs:subClassOf rdf:resource="C₂">	SubClassOf(C₁ C₂)
$C_1 \sqcup C_2$	<owl:unionOf>	unionOf(C₁ C₂)
$C_1 \sqcap C_2$	<owl:intersectionOf>	intersectionOf(C₁ C₂)
$C \equiv \{i_1, i_2\}$	<owl:oneOf>	oneOf(i₁ i₂)
r	<owl:ObjectProperty rdf:ID="r">	ObjectProperty(r)
$\geqslant 1 r \sqsubseteq C_1$	<rdfs:domain rdf:resource="C₁">	domain(C₁)
$\top \sqsubseteq \forall r.C_2$	<rdfs:range rdf:resource="C₂">	range(C₂)
a	<owl:DatatypeProperty rdf:ID="a">	DatatypeProperty(a)
$\geqslant 1 a \sqsubseteq C$	<rdfs:domain rdf:resource="C">	domain(C)
$\top \sqsubseteq \forall a.D$	<rdfs:range rdf:resource="D">	range(D)
$r.C$	<owl:Restriction>	restriction(r)
$\forall r.C$	<owl:allValuesFrom rdf:resource="C">	allValuesFrom(C)
$\exists r.C$	<owl:someValuesFrom rdf:resource="C">	someValuesFrom(C)
$\exists r.\{i\}$	<owl:has Value rdf:resource="i">	values(i)
i	<C rdf:ID="i">	Individual(i type(C))

Tabelle 5.1: Wesentliche Artefakte in OWL-DL
(siehe Baader, Horrocks und Sattler 2004)

Die jeweilige XML-basierte OWL-Syntax ist teilweise nur verkürzt dargestellt. Die dritte Spalte enthält dagegen in vollständiger Form die leichter lesbare OWL-Abstract-Syntax (siehe W3C 2004a). Um nun die Technologierisiko-Ontologie sowie die Transformation innerhalb des Prototyps verwenden zu können, wurden sie entsprechend Tabelle 5.1 in OWL-DL implementiert. Auch das im Rahmen des Fallbeispiels in Kapitel 6 erstellte bankspezifische Technologierisiko-Modell sowie die transformierten Simulationsmodelle sind in OWL-DL umgesetzt.

Die vollständige Technologierisiko-Ontologie (`trm.owl`) ist in Anhang I enthalten. Zur Darstellung wird hier aus Gründen der Übersichtlichkeit die OWL-Abstract-Syntax der XML-basierten Schreibweise vorgezogen. Zusätzlich zu den Ausdrücken `EquivalentClasses` und `SubClassOf` finden sich alternativ auch die Ausdrücke `complete` beziehungsweise `partial`.

5.3 Modelltransformation

Für die automatische Überführung des Technologierisiko-Modells eines konkreten Kreditinstitutes (`tmodel.owl`) in ein auf funktionalen Abhängigkeiten basierendes Simulationsmodell (`sim_n.owl`) werden formale Überleitungsregeln festgelegt. Diese bilden die Konzepte der Technologierisiko-Ontologie auf das Modell zur Quantifizierung ab. So können Änderungen in der IT-Landschaft direkt in das Simulationsmodell zur Quantifizierung übertragen werden.

Für diese Transformation in das Simulationsmodell wird das Konzept der Ontology Views verwendet. Allgemein beschreibt der Begriff eine neue, veränderte Sicht auf eine bereits existierende Ontologie, unabhängig von Implementierungsdetails. Innerhalb einer solchen Sicht können typische Operationen klassischer Datenbankanfragen (siehe Kemper und Eickler 1999) wie zum Beispiel die Selektion, Projektion oder Vereinigung durchgeführt werden. Die Selektion einzelner Konzepte dient der Reduktion der Betrachtung auf ausgewählte, für eine bestimmte Aufgabe benötigte Strukturen (vgl. Noy und Musen 2004, S.713f.). Auch können über die Einführung neuer Restriktionen bestimmte Individuen eines Konzepts selektiert werden. Über die Projektion von Konzepten können Zusammenhänge einer Ontologie in eine alternative Darstellung überführt werden, die einem neuen fachlichen Verständnis entspricht (vgl. Volz, Oberle und Studer 2003, S.1168f.). Die Vereinigung mehrerer Konzepte zu einem neuen wird verwendet, um bestimmte Aspekte der Ontologie zusammenzufassen.

Um eine quantitative Sicht auf das Kreditinstitut zu erhalten, werden auf der Basis der Technologierisiko-Ontologie neue Konzepte definiert. Zusätzlich werden bestehende Konzepte erweitert (vgl. Abbildung 5.3). Über das Reasoning kann dann das bankspezifische Technologierisiko-Modell in das Simulationsmodell überführt werden.

Das Mapping der Konzepte (❶) stellt die technische Umsetzung der in Kapitel 4.3 (vgl. auch Formel 4.8-4.11; 4.14-16; 4.21-4.23) beschriebenen zweistufigen Transformation (vgl. Abbildung 4.3) der Technologierisiko-Ontologie über das Modell funktionaler Abhängigkeiten in das allgemeine Simulationsmodell dar. Das Mapping besteht aus der Anwendung von Selektionen und Projektionen sowie der Bildung von Vereinigungen:

- Die Projektion erfolgt über die Einführung neuer, äquivalenter (`EquivalentClasses`) Konzepte. Hierdurch wird zum Beispiel das Konzept *ApplicationSystem* auf das Konzept *Asset* abgebildet.
- Die Selektion basiert ebenso auf der Beschreibung neuer Konzepte, die über eine Restriktion (`allValuesFrom`) bereits existierender Konzepte gebildet wird. So werden beispielsweise nur die Zustände (*State*) eines *Riskfactor* nicht jedoch die eines *Asset* zu *Input* transformiert.
- Die Vereinigung mehrerer Konzepte zu einem neuen erfolgt über die Zusammenführung (`unionOf`) der Ausgangskonzepte. Ein Beispiel stellt die Vereinigung von *ITComponent* und *ITManagementTask* zum neuen Konzept *Riskfactor* dar.

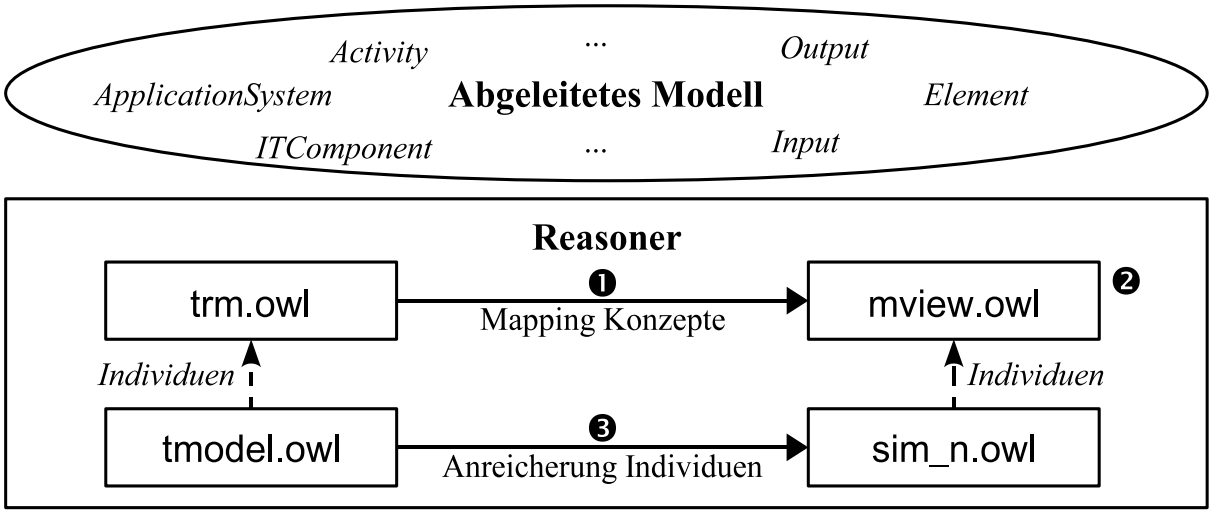

Abbildung 5.3: Gemeinsames Modell

Die Erweiterung der Konzepte (❷) *Input*, *Element* und *Output* mit dem Attribut *formula* zur Speicherung der Formeln erfolgt über die Einführung einer `DatatypeProperty` innerhalb von `mview.owl`.

Die konkrete Anreicherung (❸) der Individuen erfolgt direkt in `sim_n.owl`. Hier werden den Individuen die in Kapitel 4.3 festgelegten zufälligen Einflussgrößen, funktionalen Zusammenhänge und Verlustfunktionen (vgl. Formeln 4.12, 4.13) als Formelattribut zugewiesen.

Eine vollständige Darstellung des Ontology Views zur Transformation der Konzepte des Technologierisiko-Modells in das Simulationsmodell findet sich in Anhang II. Entsprechend der Darstellung der Technologierisiko-Ontologie wird hierfür die OWL-Abstract-Syntax verwendet.

Zusätzlich zu den Konzepten müssen auch die in der Technologierisiko-Ontologie definierten Relationen in das Simulationsmodell abgebildet werden. Aufgrund der in OWL fehlenden Möglichkeit, Relationen zu vereinigen oder zu verketten, werden solche Zusammenhänge über die Anfragesprache SPARQL ausgewertet. So können beispielsweise die Beziehungen zwischen *ITComponent* oder *ITManagementTask* und den *ApplicationSystem* über folgenden Ausdruck zu einer Relation zwischen *Riskfactor* und *Asset* zusammengefasst werden:

```
SELECT ?from ?to WHERE
  {{?from influence ?to} union
   {?from form ?to}}
```

Zusammenfassend besteht die Transformation der Technologierisiko-Ontologie in das Simulationsmodell aus den in einem Ontology View beschriebenen Mappings und Anreicherungen sowie einzelnen Anfragen in SPARQL.

5.4 Simulation

Auf Basis des jeweiligen bankspezifischen Simulationsmodells (`sim_n.owl`) wird abschließend die Simulation durchgeführt. Um das Risikopotential quantifizieren und analysieren zu können, muss aus dem Simulationsmodell zunächst Java Code generiert und dieser dann ausgeführt werden. Im Folgenden sind die wichtigsten technischen Aspekte der Code-Generierung, der Durchführung der Simulation und der Analyse der Ergebnisse dargestellt.

5.4.1 Code-Generierung

Um das Simulationsmodell ausführbar zu machen, wird aus den in der Datei `sim_n.owl` enthaltenen Individuen Java Code generiert. Hierzu wird das Simulationsmodell zunächst in eine Darstellung als Graph überführt. Die Individuen von *Input*, *Element* und *Output* stellen dabei die Knoten dar, die Kanten werden aus den Relationen gebildet. An dieser Stelle erfolgt nun eine statische Bindung der Konzepte an die drei Java Klassen `Input`, `Element` und `Output`. Diese stellen Methoden zum Zugriff auf die enthaltenen Formeln zur Verfügung. Hierunter fallen insbesondere Methoden zur syntaktischen Überprüfung der Formeln sowie zur Generierung des jeweiligen Java Codes. Im Detail erfolgt die Erzeugung des Simulationscodes entsprechend folgendem dreistufigen Schema:

1. Über eine topologische Sortierung des Graphen (vgl. Cormen, Leiserson und Rivest 1998, S.485f.) wird zunächst die Ausführungsreihenfolge der Knoten ermittelt. Eventuelle Zyklen werden hierbei erkannt und die Simulation abgebrochen.
2. Vor der Erzeugung des Java Codes werden die Formeln zunächst über reguläre Ausdrücke (vgl. Abbildung 5.4) syntaktisch geprüft. Zusätzlich wird sichergestellt, dass in den Formeln nur benachbarte Knoten (zu denen also eine gültige Relation besteht) referenziert werden. Im Fehlerfall wird die Simulation abgebrochen.
3. Die anschließende Überführung in Java Code basiert auf einem vorgefertigten Template. Hierzu werden die Formeln der Individuen als Java Code gelesen und an eine vordefinierte Stelle im Template kopiert.

Die in den regulären Ausdrücken referenzierten Funktionen `bernoulli`, `lognormal`, `gamma` und `weibull` sind innerhalb des Templates als Methoden definiert und kapseln den Zugriff auf die den Verteilungen entsprechenden Zufallsvariablen.

```
Input.formula:     bernoulli\(\d+(\.\d+)?\)
Element.formula:   step\(\d+(\.\d+)?
                   (-[a-zA-Z]*_[a-zA-Z]*)+\)
Output.formula:    (lognormal|gamma|weibull)
                   \(\d+(\.\d+)?,\d+(\.\d+)?\)
```

Abbildung 5.4: Reguläre Ausdrücke der Formeln

5.4.2 Durchführung

Die eigentliche Simulation läuft gemäß dem in Kapitel 4.3.5 beschriebenen Pseudo-Code ab. Entscheidend für die Durchführung der Simulation ist die Wahl des Zufallszahlengenerators und des Algorithmus zur Erzeugung der Verteilungen. Um die Belastbarkeit der Ergebnisse sicherzustellen, ist ein möglichst hoher Grad an Zufälligkeit erforderlich. Das Laufzeitverhalten der Simulation spielt aufgrund des Einsatzes von direkt kompiliertem Java Code für den Prototyp eine eher untergeordnete Rolle.

In dieser Arbeit wird die in Java implementierte SSJ Bibliothek zur Generierung der Zufallszahlen verwendet. Hierin sind unterschiedliche Generatoren für Pseudo-Zufallszahlen enthalten. Diese unterscheiden sich im Hinblick auf Periodenlänge, Geschwindigkeit der Zufallszahlenerzeugung sowie Grad der Zufälligkeit. Tabelle 5.2 gibt einen Überblick der in SSJ enthaltenen Implementierungen bekannter Generatoren. Es sind jeweils die Periodenlänge sowie die für die Generierung einer festen Anzahl von Zufallszahlen benötigte Zeit aufgeführt.

Implementierung	Algorithmus	Periodenlänge	Zeit
GenF2w32	Linear Congruential Generator	2^{800}	62*s*
LFSR113	Composite Linear Feedback Shift	2^{113}	51*s*
MRG32k3a	Combined Multiple Recursive	2^{191}	109*s*
MT19937	Mersenne Twister	2^{19937}	56*s*

Tabelle 5.2: Vergleich Zufallszahlengeneratoren
(siehe L'Ecuyer 2005, Zeiten für 10^9 Zufallszahlen auf 32-Bit 2100Mhz Athlon)

Für eine detaillierte Darstellung der einzelnen Algorithmen wird auf die Literatur verwiesen (vgl. Knuth 1998, S.10ff.; Matsumoto und Nishimura 1998; L'Ecuyer 2006). Im Hinblick auf die Periodenlänge eignen sich sämtliche oben genannten Implementierungen für den hier entwickelten Prototyp. Eine Analyse der Zufälligkeit (siehe L'Ecuyer 2001) zeigt ein gutes Verhalten bei der MT19937 und der MRG32k3a Implementierung. Da das Laufzeitverhalten für den Prototyp eine untergeordnete Rolle spielt, wird zur Generierung der Zufallszahlen die langsamste jedoch auch mit dem höchsten Maß an Zufälligkeit versehene Implementierung MRG32k3a gewählt. Die Transformation der über den Zufallszahlengenerator erzeugten Gleichverteilung in die jeweilige im Simulationsmodell spezifizierte Verteilung erfolgt über die Inversionsmethode.

5.4.3 Analyse

Sowohl die numerische als auch die graphische Analyse der Simulationsergebnisse erfolgt mittels R-Skripten. Für die Berechnung der Risikomaße VaR und CVaR wird das RiskMetrics-Paket (siehe Rmetrics 2006) verwendet. Entscheidend für eine graphische Darstellung der Ergebnisse ist die Überführung der diskreten Realisationen in eine stetige Dichtefunktion. Hierzu wird die Dichtefunktion mittels einer Kernel-Density-Function approximiert (siehe Wand und Jones 1995). Von den unterschiedlichen möglichen Kernen wird für den Prototyp der Epanechnikov-Kern verwendet. Dieser beruht auf einer intervallweisen Annäherung der Dichtefunktion über eine Beta (2,2)-Verteilung.

Die Berechnung der geschätzten Dichtefunktion erfolgt im Prototyp über das R-Paket KernSmooth (siehe Wand und Ripley 2005). Hierbei erfolgt die Annäherung über die Auswertung von 200 Stützstellen über die gesamte Bandbreite der simulierten Verluste.

Die Abbildung 5.5 zeigt einen Screenshot des Prototyps nach Auswertung eines exemplarischen Simulationsmodells, welches auf der im Fallbeispiel in Kapitel 6 entwickelten Systemlandschaft basiert (vgl. Abbildung 6.4). Im linken oberen Bereich wird die Graphendarstellung des aus der Ontologie erzeugten Simulationsmodells, bestehend aus Inputs (Zustände der Risikofaktoren), Elementen (Zustände der Assets) und Outputs (Verlustfunktionen), angezeigt. Die bestehenden Abhängigkeiten werden als gerichtete Kanten dargestellt. Im rechten oberen Bereich befindet sich die angenäherte Dichtefunktion des Gesamtverlustpotentials. Zudem werden in einem Statusfenster der Fortschritt der Simulation sowie nach Beendigung die Risikomaße VaR und CVaR ausgewiesen.

5.5 Zusammenfassung

Die beschriebene Anwendung stellt eine prototypische Implementierung der in Kapitel 4.3 entwickelten Methode zur Quantifizierung auf Basis des in Kapitel 3.2 vorgeschlagenen Modells operationeller Technologierisiken dar. Die Motivation für die Umsetzung eines Prototyps war zum einen die Demonstration der technischen Machbarkeit der vorgeschlagenen Methode zur Risikoquantifizierung, zum anderen sollte die Voraussetzung dafür geschaffen werden, die Ontologie-zentrierte Simulation im Rahmen eines Fallbeispiels in Kapitel 6 durchzuführen.

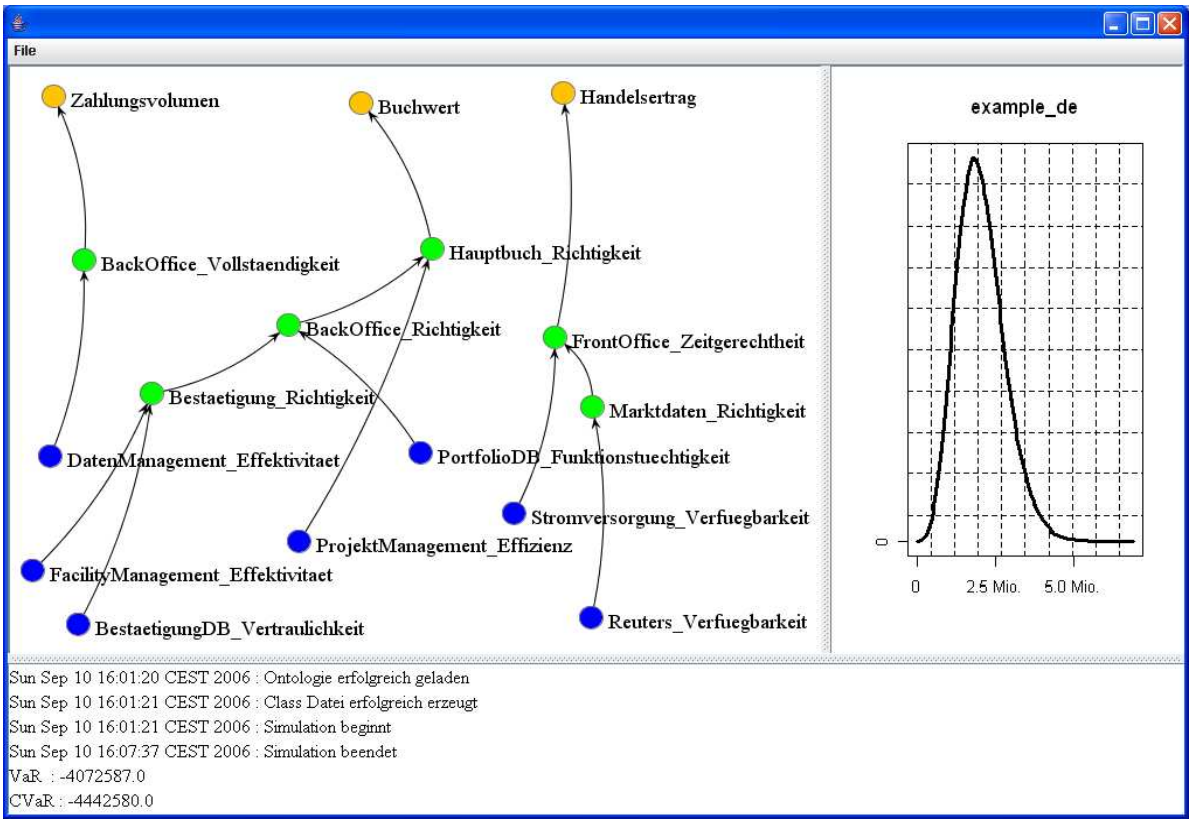

Abbildung 5.5: Screenshot Prototyp

Wichtig ist in diesem Zusammenhang, dass bei der Entwicklung des Prototyps sowohl die relevanten Gesichtspunkte des Modells als auch die der Methode implementiert werden:

- Das in Kapitel 3.2 in DL beschriebene Verständnis operationeller Technologierisiken kann vollständig in OWL-DL umgesetzt werden (vgl. Tabelle 5.1). So werden durch den Prototyp sämtliche Konzepte, Relationen und Restriktionen berücksichtigt.
- Die in Kapitel 4.3 vorgestellte Ontologie-zentrierte Simulation zeichnet sich dadurch aus, dass das IT-Umfeld der Bank erst auf Basis der Technologierisiko-Ontologie modelliert und dann automatisch in ein auf funktionalen Abhängigkeiten basierendes Simulationsmodell überführt wird. Durch das Konzept der Ontology Views sowie SPARQL-Abfragen wird die in Kapitel 4.3.1 bis 4.3.4 beschriebene Transformation vollständig umgesetzt. Die für die Darstellung der funktionalen Abhängigkeiten benötigten Ausdrücke können über das eingeführte Formelattribut erfasst werden. Damit kann das aus Input, Element und Output bestehende Simulationsmodell automatisch in ausführbaren Java Code übersetzt werden.

Der Prototyp der Ontologie-zentrierten Simulation erfüllt somit die sich jeweils aus dem Modell und der Methode ergebenden Anforderungen. Abschließend ist aber auch anzumerken, dass aufgrund der ausschließlich prototypischen Implementierung einzelne, für den technischen „proof of concept“ zu vernachlässigende Aspekte, unberücksichtigt bleiben:

- Eine genaue Betrachtung des Laufzeitverhaltens der Simulation wird nicht vorgenommen, es kann jedoch in der Regel ein linearer Zusammenhang zwischen Anzahl der Iterationen und Laufzeit unterstellt werden. Für die im Fallbeispiel durchgeführten Simulationen (vgl. Kapitel 6.3) kann der Faktor Zeit vernachlässigt werden. Für komplexe Modelle (hohe Anzahl Knoten und Kanten) sind zwangsläufig längere Laufzeiten zu erwarten. Zur Optimierung des Laufzeitverhaltens kann dann die Simulation auf mehrere Rechner verteilt werden.
- Eine graphische Benutzeroberfläche zur Modellierung des Technologie-Umfelds des Kreditinstitutes ist nicht Bestandteil des Prototyps. Hierfür kommt die Einbindung eines auf Graphen basierenden Editors in Frage.
- Die technischen Auswirkungen von Erweiterungen oder Änderungen in der Technologierisiko-Ontologie und die Übertragung auf eine vollständig unterschiedliche Domäne (z.B. Prozessrisiken) wird nicht untersucht. Hierzu wäre das festgelegte Mapping sowie in Teilen der Programmcode anzupassen.

Im folgenden Kapitel wird die prototypische Implementierung genutzt, um ein realistisches Fallbeispiel vorzustellen. In dessen Verlauf wird eine Szenario-Analyse durchgeführt, um verschiedene Alternativen der Risikoquantifizierung zu vergleichen. Die Ermittlung des Risikopotentials auf Basis der Ontologie-zentrierten Simulation erfolgt dabei vollständig automatisiert über in OWL-Dateien gespeicherte Simulationsmodelle.

Kapitel 6
Fallbeispiel: Outsourcing im Handel

Die im Rahmen der Arbeit konzipierte und implementierte Vorgehensweise zur Quantifizierung von Technologierisiken wird in diesem Kapitel verdeutlicht und auf ihre fachliche Anwendbarkeit hin untersucht. Hierzu wird ein Fallbeispiel aktueller Thematik vorgestellt. In diesem wird eine reale Entscheidungssituation des IT-Managements unterstellt, nämlich das Outsourcing eines wesentlichen Anwendungssystems im Handel einer Bank. Eingebettet in das Fallbeispiel werden mittels einer Szenarioanalyse die Stärken und Schwächen der Ontologie-zentrierten Simulation demonstriert und im Vergleich zum Standardansatz untersucht. So kann die Auswirkung verschiedener Alternativen der Quantifizierung jeweils unter Einfluss unterschiedlicher Szenarien beleuchtet werden. Das Outsourcing bietet sich für eine Gegenüberstellung der Methoden an, da es sich um ein stark risikobehaftetes Szenario handelt, in welchem die Risikosensitivität eine besondere Rolle spielt. Ziel ist es jedoch nicht, das Outsourcing im Geschäftsfeld Handel generell zu analysieren, sondern ausschließlich Vor- und Nachteile beider Vorgehensweisen zur Quantifizierung aufzuzeigen.

Nachfolgend werden zunächst die Motivation für das Fallbeispiel aufgegriffen und relevante Rahmenbedingungen erörtert. Ferner wird der durch die MaRisk vorgegebene Prozessaufbau im Geschäftsfeld Handel als Grundlage für das Fallbeispiel dargestellt. Die Anwendung der Ontologie-zentrierten Vorgehensweise erfolgt auf der Basis möglichst allgemeingültiger Annahmen. So wird für das Simulationsmodell und die Auswertung der Ergebnisse ein idealtypisches Kreditinstitut entsprechend der Struktur deutscher Großbanken unterstellt.

6.1 Motivation und Ausgangslage

Um die zu untersuchenden Szenarien und Alternativen in einen anwendungsbezogenen Rahmen einzubetten, wird die Betrachtung auf ein konkretes Geschäftsfeld bei Kreditinstituten eingegrenzt. So kann die Darstellung des Fallbeispiels anhand eines konkreten Anwendungsbereichs erfolgen. Die bisher im

Rahmen der Basel II Einführungen erhobenen Daten zeigen ein je nach Geschäftsfeld deutlich variierendes operationelles Risikopotential. Hier wird bewusst ein Geschäftsfeld mit ausgeprägtem Risikoprofil gewählt, in welchem zudem die Informationstechnologie eine besondere Bedeutung hat. Im Folgenden werden zuerst die Besonderheiten im Geschäftsfeld Handel charakterisiert und dann die spezifischen Herausforderungen des Outsourcings verdeutlicht.

6.1.1 Geschäftsfeld Handel

Die Unterschiede im operationellen Risikopotential werden auch durch die Verwendung spezifischer β-Faktoren im Standardansatz reflektiert (vgl. Tabelle 4.3). So wird beispielsweise das Risiko in der Vermögensverwaltung generell mit 12%, in der Unternehmensfinanzierung hingegen mit 18% abgeschätzt. Dieses unterschiedliche Risikoprofil ist jedoch nicht zwangsläufig bankenübergreifend gleichmäßig (vgl. Fontnouvelle und Rosengren 2004, S.12ff.).

Für dieses Fallbeispiel wird das Geschäftsfeld Handel ausgewählt, das wesentliche Kerngeschäftsprozesse des Bankbetriebs beinhaltet (vgl. Lamberti 2004, S.372). Dies lässt sich auch mit dem ausgeprägten operationellen Risikopotential dieses Geschäftsfeldes begründen, was sich in einer hohen regulatorischen Kapitalanforderung nach dem Standardansatz (β = 18%) niederschlägt. Die Tabelle 6.1 zeigt den im Vorfeld der Basel II Einführung ermittelten Anteil der Verluste im Geschäftsfeld Handel an den gesamten Verlusten.

	QIS II Tranche 2		**LDCE 2002**		**LDCE 2004**	
	Mio. EUR	Anzahl	Mio. EUR	Anzahl	Mio. EUR	Anzahl
Im Handel	500	1.334	1.163	5.132	742	1.335
Gesamt	2.613	27.371	7.796	47.269	8.643	18.371
% Anteil	19,1	4,9	14,9	10,9	8,6	7,3

Tabelle 6.1: Anteil der Verluste im Geschäftsfeld Handel

Durchgeführte Analysen zeigen ferner, dass Verluste im Handel seltener auftreten, aber die jeweilige Verlusthöhe anderer Geschäftsfelder überschreiten (vgl. Fontnouvelle et al. 2003, S.8). Ein letzter Grund für die Auswahl des Geschäftsfeld Handel liegt in der überdurchschnittlichen Abhängigkeit von Informationstechnologie. Besonders das wachsende Handelsvolumen mit komplexen Derivaten (vgl. Abbildung 6.1) stellt aufgrund der geringen Standardisierung hohe Anforderungen an die unterstützenden Anwendungssysteme.

Dem Verständnis von Basel II entsprechend umfasst das Geschäftsfeld Handel sowohl die Kundengeschäfte (Maklergeschäft für Großkunden), als auch den klassischen Eigenhandel, das Market Making sowie das Treasury (vgl. Basel II, Anhang 8). Damit geht das Verständnis über den Eigenhandel im engeren Sinn hinaus, der nur die *„[...] an den nationalen oder internationalen Märkten (inkl. den OTC- und Interbanken-Märkten) abgegebene Endleistungen eines Kreditinstituts [umfasst], die nicht im Auftrag eines Kunden vorgenommen werden und nicht der Bilanzstrukturpolitik dienen [...]“* (Morgenstern 2004, S.6f.). Sämtliche Formen des Handels können grundsätzlich im Bereich von Wertpapieren, (OTC)-Derivaten oder Edelmetallen betrieben werden.

Im Standardansatz wird als Schätzer für das Risikopotential das Handelsergebnis abzüglich Refinanzierung und zuzüglich Provisionen aus Großkunden Maklergeschäft vorgeschlagen (vgl. Basel II, Anhang 8). Wesentliche Messgröße für den Anteil des (Eigen-)Handels am Gesamtergebnis ist somit der Nettoertrag aus Finanzgeschäften (HGB), auch als Handelsergebnis bezeichnet. Diese Größe ist stark volatil, was ebenso ein Indikator für das hohe Risiko in diesem Geschäftsfeld ist. Sie machte in den Jahren 1999 bis 2004 einen nicht unerheblichen Anteil des Betriebsergebnisses der deutschen Großbanken aus (vgl. Deutsche Bundesbank 2005, S.39).

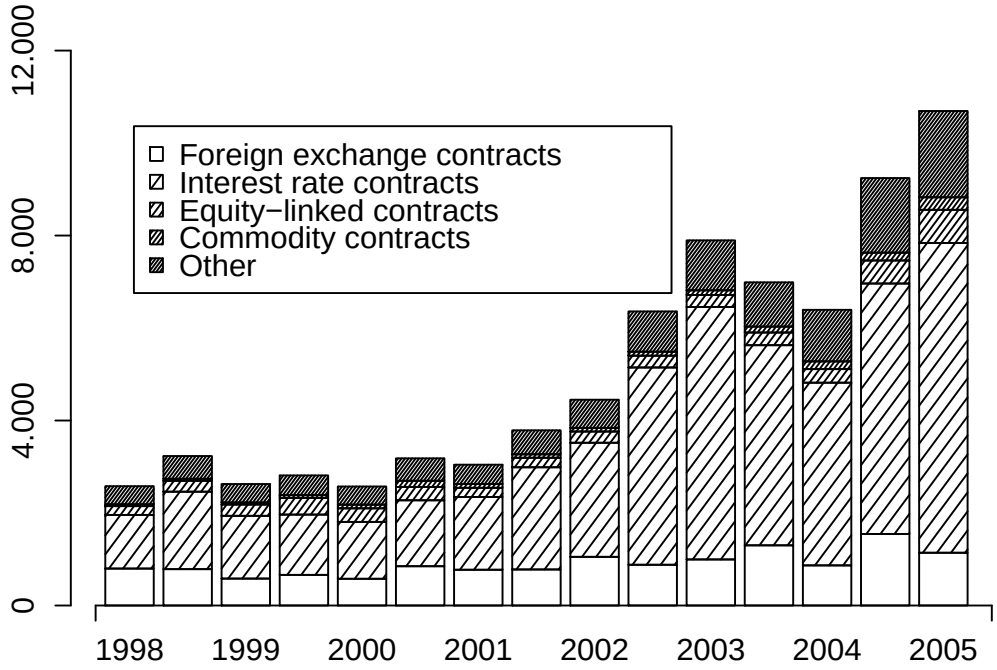

Abbildung 6.1: Marktwert OTC-Derivate (USD)
(siehe BIS 2005)

6.1.2 Outsourcing in der Kreditwirtschaft

Der zunehmende Kostendruck auf Kreditinstitute (gemessen z.B. am Aufwand-Ertrag-Verhältnis) hat auch in Deutschland zu einer Diskussion der Wertschöpfungstiefe geführt. Obwohl das Verhältnis zwischen Aufwand und Ertrag über alle deutschen Banken hinweg in den letzten Jahren im Durchschnitt gesunken ist (vgl. Abbildung 6.2), wird bei den Großbanken im europäischen Vergleich weiterhin Aufholbedarf gesehen. Unter dem Oberbegriff der Industrialisierung der Kreditwirtschaft wird eine Verringerung der Wertschöpfungstiefe bei Kreditinstituten diskutiert, um eine Fokussierung auf die Kernkompetenzen voranzutreiben. Dies trifft in hohem Maße auch auf die deutschen Großbanken entsprechend der Klassifikation der deutschen Bundesbank zu.

Das Outsourcing stellt gerade im Bereich der IT-gestützten Prozesse von Banken eine häufig genutzte Alternative zur Reduktion der Wertschöpfungstiefe dar, um Kostenvorteile zu erlangen. Nicht zuletzt deshalb ist das Outsourcing bei Kreditinstituten ein aktuelles Thema. Eine Studie der europäischen Zentralbank hat ergeben, dass nahezu alle befragten Banken Auslagerungen von Teilbereichen oder Prozessen vorgenommen haben (vgl. ECB 2004, S.26).

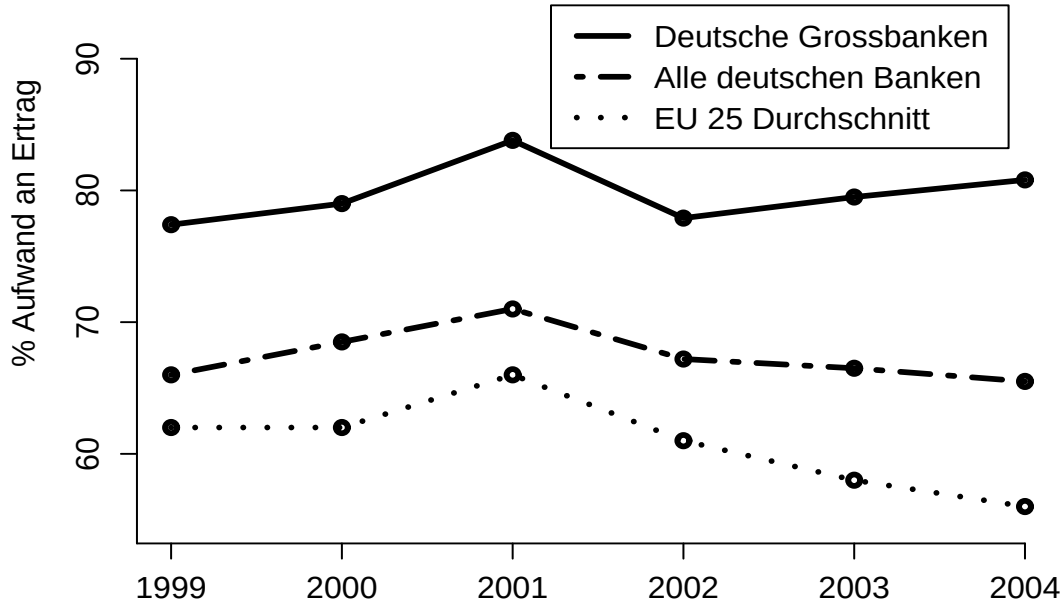

Abbildung 6.2: Entwicklung Aufwand-Ertrag-Verhältnis
(siehe Deutsche Bundesbank 2005; ECB 2005a)

In einem Vorschlag definiert der Basler Ausschuss den Begriff Outsourcing aus aufsichtsrechtlicher Perspektive *„[...] as a regulated entity's use of a third party (either an affiliated entity within a corporate group or an entity that is external to the corporate group) to perform activities on a continuing basis that would normally be undertaken by the regulated entity, now or in the future.“* (BCBS 2005, S.4)

Im europäischen Rahmen wird die Kostenreduktion als wesentliche Triebfeder für Outsourcing-Projekte angesehen (vgl. ECB 2004, S.28). Des Weiteren spielen jedoch auch technologische Verbesserungen sowie eine Fokussierung auf die eigentlichen Kernbereiche eine zentrale Rolle. Beispiele für Outsourcing von Informationstechnologie oder Geschäftsprozessen sind die Verlagerung des IT-Betriebs der Deutschen Bank an IBM oder die Gründung von VR-Kreditwerk zur Abwicklung von Krediten im genossenschaftlichen Sektor. Im Wesentlichen werden nur unterstützende Aktivitäten ausgelagert. Die Kernkompetenzen zur Erlangung von Wettbewerbsvorteilen dagegen werden intern ausgebaut.

Wie bereits in der obigen Definition angedeutet, kann das Outsourcing in verschiedenen Organisationsformen durchgeführt werden. Hierbei kommt der gesellschaftsrechtlichen Verflechtung eine besondere Bedeutung zu. Es können beispielsweise die Gründung einer eigenen Tochtergesellschaft, die Übertragung auf einen externen Dritten oder die Bildung einer Kooperation unterschieden werden (vgl. Foit 2005, S.163ff.). Die häufigste Form ist die Auslagerung an eine separate Gesellschaft, die entweder innerhalb des Konzerns oder als externes Unternehmen (im eigenen Land) besteht (vgl. ECB 2004, S.26). Wichtig beim Outsourcing ist, dass der abgeschlossene Vertrag möglichst präzise Regelungen zur Leistungserbringung enthält (vgl. Foit 2005, S.176ff.). Durch Service Level Agreements (SLA) wird die benötigte Qualität, beispielsweise im Hinblick auf Verfügbarkeit, geregelt. Bei einem Abweichen von der Vorgabe kann darin auch eine Ausgleichszahlung vereinbart werden.

Das Outsourcing ist selbst wiederum mit Risiken verbunden (vgl. Foit 2005, S.190ff.). Als wesentliche Risikopotentiale im Zusammenhang mit Outsourcing werden von Banken der Verlust von Kontrolle, eine Zunahme bestimmter operationellen Risiken sowie die Reduktion eigener Qualifikationen gesehen (vgl. ECB 2004, S.29). Zusätzlich steigt auch die Bedeutung der rechtlichen Risiken.

Insgesamt kann festgehalten werden, dass Outsourcing eine Möglichkeit zur Kostenreduktion und zur Steigerung der Qualität einzelner Prozessschritte darstellt, die in verschiedenen Organisationsformen durchgeführt werden kann. Outsourcing ist jedoch selbst mit neuen, inhärenten Risiken behaftet.

6.1.3 Vorgehensweise und Datengrundlage

Um die Wirkungsweise der Ontologie-zentrierten Simulation auf Technologierisiken zu verdeutlichen, wird ein an idealtypische sowie aufsichtsrechtlich vorgegebene Bankstrukturen angelehntes Fallbeispiel im Handel betrachtet. Grundlage der Betrachtung stellt eine Szenarioanalyse dar, in welcher zwei unterschiedliche Alternativen der Quantifizierung verglichen werden:

1. Quantifizierung der Risiken mittels Standardansatz
2. Quantifizierung der Risiken mittels Ontologie-zentrierter Simulation

Die Szenarien reichen dabei von dem Eigenbetrieb sämtlicher Anwendungssysteme bis zu einer Auslagerung eines wesentlichen Systems der Abwicklung an einen externen Dienstleister mit beziehungsweise ohne Eigenkapitalbeteiligung. Im Rahmen des Fallbeispiels sollen jedoch nicht generell Vor- und Nachteile eines Outsourcing-Vorhabens untersucht, sondern ausschließlich die Auswirkung der alternativen Ansätze zum Risikomanagement analysiert werden. In einer Sensitivitätsanalyse werden abschließend die Auswirkungen verschiedener Simulationsparameter sowie unterschiedlicher Annahmen bezüglich des Standardansatzes beleuchtet.

Um das Fallbeispiel möglichst allgemeingültig zu halten, werden bewusst keine bankspezifischen Einschränkungen gemacht. Erstens wird der Analyse ein allgemeiner und idealtypischer Prozessaufbau im Handel zugrunde gelegt, wie er durch die MaRisk für alle Kreditinstitute vorgeschrieben ist. Zweitens wird ein Vergleich mit dem Standardansatz gezogen. Drittens entstammen die für die quantitative Analyse verwendeten Zahlen veröffentlichten Quellen, so dass keine Einschränkung in der Darstellung vorgenommen werden muss. Für das Fallbeispiel werden im Wesentlichen folgende Quellen herangezogen:

Quelle	Daten	Jahr
QIS II (siehe BCBS 2002)	Durchgeführt von der RMG, auf Basis einzelner Verlustereignisse, 1998-2000, 30 internationale Banken	2002
LDCE 2002 (siehe BCBS 2003c)	Durchgeführt von der RMG, Erweiterung der QIS II, 2001, 89 internationale Banken	2002
LDCE 2004 (siehe Fed 2005)	US Federal Bank, auf Basis einzelner Verluste, bis einschließlich 2004, 27 US-amerikanische Banken	2004
Ertragslage (siehe Deutsche Bundesbank 2005)	Ertragslage deutscher Banken im Jahr 2004	2005

Tabelle 6.2: Herangezogene Datenquellen

Um den Abgleich mit dem Standardansatz durchführen zu können, muss zum einen ein Schätzer für den Bruttoertrag im Handel verwendet werden. Hierzu dient das Handelsergebnis entsprechend der Statistik der deutschen Bundesbank (vgl. Deutsche Bundesbank 2005).

Zum anderen muss der Anteil der Technologierisiken im Geschäftsfeld Handel geschätzt werden. Da die offen zugänglichen Daten kein genaues Aufschlüsseln der Verlustereignisse zulassen, werden die Technologierisiken auf Ebene der obersten Ereigniskategorie geschätzt. Als wichtige Datenquelle wird die LDCE 2002 aufgefasst (vgl. McNeil, Frey und Embrechts 2006, S.505). Hieraus werden die für Technologierisiken wesentlichen Ereigniskategorien abgeleitet (vgl. Tabelle 6.3; Tabelle 4.4). Die beiden Kategorien Geschäftsunterbrechung und Systemausfälle sowie Abwicklung, Lieferung und Prozessmanagement werden addiert. Die in der Kategorie externe betrügerische Handlungen beinhaltete Teilkategorie Systemsicherheit wird in diesem Zusammenhang als nicht bedeutend eingestuft:

Ereigniskategorie	QISII-T2	LDCE 2002	LDCE 2004
Geschäftsunterbrechung und Systemausfälle	6	17	5
Abwicklung, Lieferung und Prozessmanagement	327	698	239
Summe	333	715	244
Handel gesamt	500	1.163	742
Anteil	**67%**	**61%**	**33%**

Tabelle 6.3: Anteil Technologierisiken im Eigenhandel
(Beträge in Mio. EUR / USD)

Die Anteile der Technologierisiken (gemessen an der Verlusthöhe) an den operationellen Risiken im Handel unterscheiden sich je nach Datenquelle deutlich. Es zeigt sich jedoch, dass die Technologierisiken im Handel überdurchschnittlich (mehr als 25% aller operationellen Risiken) vorhanden sind. Besonders die aus öffentlichen Quellen zusammengestellten Pool-Daten zeigen in Abhängigkeit vom Ursprungsland deutliche Abweichungen. Auf die spezifischen Besonderheiten externer Daten wurde bereits in Kapitel 4.2.2.c hingewiesen. Weitere Analysen externer Pool-Daten finden sich in Cummins, Lewis und Wei 2004 oder Rachev, Chernobai und Menn 2004.

6.2 Prozessualer Aufbau des Handelsgeschäfts

Für die Entwicklung eines konkreten Fallbeispiels wird ein standardisierter Handelsprozess bei Kreditinstituten verwendet. Der dargestellte Aufbau ist dabei an die deutschen MaRisk (vgl. Kapitel 2.2.4) angelehnt. Zentraler Grundsatz dieser Vorschriften ist die klare Funktionstrennung des eigentlichen Handelsbereichs – im Sinne des Geschäftsabschlusses – von der weiteren Abwicklung sowie dem Risikocontrolling:

„Maßgeblicher Grundsatz für die Ausgestaltung der Prozesse im Handelsgeschäft ist die klare aufbauorganisatorische Trennung des Bereichs Handel von den Funktionen des Risikocontrollings sowie der Abwicklung und Kontrolle bis einschließlich der Ebene der Geschäftsleitung.“ (MaRisk, BTO2.1.1)

Darüberhinaus wird gefordert, auch die bilanzielle Abbildung der getätigten Handelsgeschäfte in einem separaten Teilbereich zu organisieren:

„Das Rechnungswesen, insbesondere die Aufstellung der Kontierungsregeln sowie die Entwicklung der Buchungssystematik, ist in einer vom Markt und Handel unabhängigen Stelle anzusiedeln.“ (MaRisk, BTO7)

Im Folgenden werden die vier wesentlichen Teilbereiche Handel, Abwicklung, Controlling und Rechnungswesen mit ihren jeweiligen finanziellen Einflussgrößen (vgl. Abbildung 6.3) vorgestellt und die aufsichtsrechtlich relevanten Tätigkeiten und Anforderungen zusammengefasst.

Der Handel ist - im Rahmen einer bankweiten Handelsstrategie - zuständig für die Entscheidung über Art und Höhe der durchzuführenden Geschäfte sowie deren konkreten Abschluss mit dem jeweiligen Kontrahenten. In diesem Sinne verantwortet der Teilbereich Handel in einem hohen Maß das im gesamten Handelsprozess realisierte Ergebnis. Bei der Durchführung der Handelsgeschäfte ist besonders darauf zu achten, dass diese zu marktgerechten Bedingungen (z.B. keine Nebenabsprachen) durchgeführt werden (vgl. MaRisk, BTO2.2.1.2). Ferner sind sämtliche Geschäfte unverzüglich mit allen erforderlichen Informationen (z.B. Stückzahl oder Kurs) zu erfassen (vgl. MaRisk, BTO2.2.1.5). Wird hierzu ein Anwendungssystem verwendet, muss sichergestellt sein, dass jeder Händler nur unter seiner Benutzerkennung Geschäfte erfassen kann und diese mit genauer Uhrzeit und ID versehen werden (vgl. MaRisk, BTO2.2.1.6). Geschäfte, die nach Erfassungsschluss in der Abwicklung eingegeben werden, sogenannte Spätgeschäfte, sind unbedingt zu berücksichtigen, wenn sich hieraus nennenswerte Änderungen am Risiko ergeben (vgl. MaRisk, BTO2.2.1.7).

Der Teilbereich Abwicklung ist direkt dem Handel nachgeordnet und übernimmt durch die Abstimmung der getätigten Geschäfte eine wichtige Kontrollfunktion innerhalb des Handelsprozesses. Darüber hinaus werden die resultierenden Ein- und Auszahlungen abgerechnet, wodurch das gesamte Zahlungsvolumen des Handels in die Verantwortlichkeit der Abwicklung fällt. Um die Geschäfte zu kontrollieren, müssen von der Abwicklung unverzüglich Geschäftsbestätigungen erstellt und an die Abwicklung des Kontrahenten versandt werden (vgl. MaRisk, BTO2.2.2.2). Diese müssen alle relevanten Geschäftsdaten enthalten. Ferner ist die Abwicklung verpflichtet dafür Sorge zu tragen, dass die geführten Geschäfte vollständig und richtig vorliegen (vgl. MaRisk, BTO2.2.2.4). Dazu sollen regelmäßig Abstimmungen mit den Beständen im Handel und Rechnungswesen vorgenommen werden (vgl. MaRisk, BTO2.2.2.7).

Dem Risikocontrolling obliegt die Verantwortung, die getätigten Geschäfte im Hinblick auf das finanzielle Risiko zu bewerten, die Einhaltung der Limite sicherzustellen und die im Handel ermittelten Ergebnisse zu validieren. Hierzu ist es entscheidend, dass die Positionen unverzüglich im Risikocontrolling abgebildet werden (vgl. MaRisk, BTO2.2.3). Mindestens zu berücksichtigen sind die Adressenausfall-, die Marktpreis-, die Liquiditäts- und die operationellen Risiken. Besonders auch für die Marktpreisrisiken müssen sämtliche Handelsgeschäfte täglich bewertet werden und die gesamte Risikosituation sowie die Auslastung der Limite gemeldet werden (vgl. MaRisk, BTR2.2).

Dem Rechnungswesen kommt im Rahmen des Handelsprozesses die Aufgabe zu, die getätigten Geschäfte in der Bilanz sowie der Gewinn- und Verlustrechnung abzubilden. Dabei ist besonders die richtige Ermittlung der buchhalterischen Bestände und des Ergebnisbeitrags wichtig. Hierzu schreiben die MaRisk vor, dass auf jeden Fall die Erstellung der Systematik für die Kontierung und Buchung getrennt vom Handel zu erfolgen hat (vgl. MaRisk, BTO7).

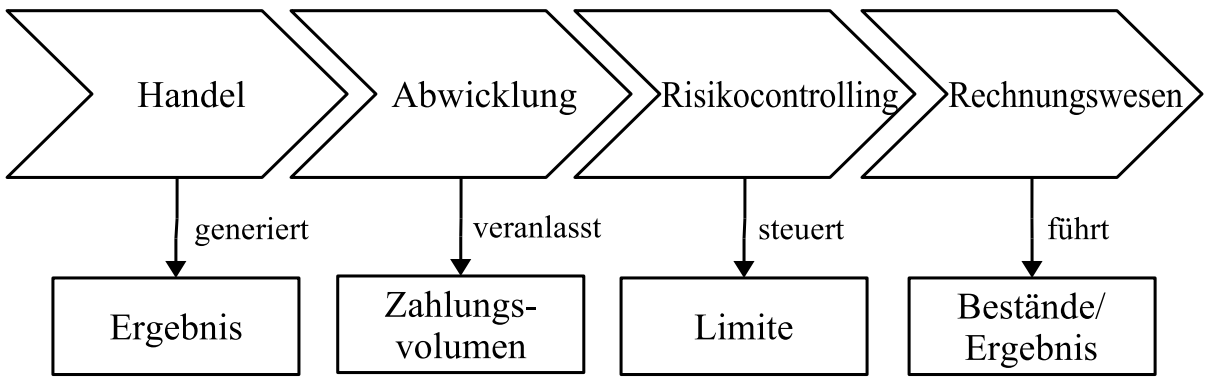

Abbildung 6.3: Wertkette im Handel

6.3 Anwendung der Ontologie-zentrierten Simulation

Um die Vorgehensweise der Ontologie-zentrierten Simulation zu verdeutlichen, wird der im vorangegangenen Kapitel 6.2 dargestellte generische Handelsprozess in eine Topologie aus Anwendungssystemen, IT-Komponenten, IT-Managementaufgaben sowie bestehenden direkten Abhängigkeiten eingebettet. Diese schematische IT-Landschaft beinhaltet somit alle beschriebenen Konstrukte des Modells. Sie stellt die Ausgangslage für das Fallbeispiel dar. Innerhalb dieser Umgebung wird anschließend das Szenario „Outsourcing des Bestätigungssystems“ simuliert. Das umfasst die Auslagerung des Anwendungssystems zur Erzeugung und Verwaltung der Bestätigungen und Gegenbestätigungen an einen externen Anbieter. Dieser kann entweder eine Tochtergesellschaft oder eine vom auslagernden Unternehmen unabhängige Gesellschaft sein.

Auf dieser Basis wird ein schematischer Vergleich zwischen der Ontologie-zentrierten Simulation und dem Standardansatz nach Basel II gezogen. Hierzu werden beide Alternativen der Risikomessung auf die unterschiedlichen Szenarien angewandt und die ermittelten Risikopotentiale einander gegenübergestellt.

6.3.1 Betrachtete Systemlandschaft

Ausgangspunkt der Betrachtung ist die Topologie der Anwendungssysteme im gesamten Handelsprozess (vgl. Abbildung 6.4). Hierin enthalten sind sechs mögliche Anwendungssysteme, die zur Durchführung der einzelnen Aufgaben innerhalb des Handels, der Abwicklung, des Risikocontrollings und des Rechnungswesens eingesetzt werden. Das Szenario einer möglichen Auslagerung an einen externen Anbieter ist in der Abbildung (schraffierte Fläche) enthalten.

Im Teilbereich Handel werden zwei Anwendungssysteme abgebildet, eine zentrale Datenbank für Marktdaten sowie die eigentliche Handelsplattform:

- Die Verwaltung sämtlicher Marktdaten, wie beispielsweise Aktienkurse, Zinssätze oder Devisenkurse, erfolgt gebündelt in einem Anwendungssystem (*Marktdaten*). Diese sind die Grundlage für Kauf- und Verkaufsentscheidungen im Handel. Um die Marktgerechtheit sicherzustellen, ist es von besonderer Bedeutung, dass die gespeicherten Daten korrekt sind.
- Die Bewertung und Durchführung der Geschäfte erfolgt in der Handelsplattform (*FrontOffice*), die auch für die Positionsführung verantwortlich ist. Besonders wichtig ist es, dass die Geschäfte zu jeder gewünschten Zeit unmittelbar getätigt werden können. Es besteht daher eine direkte Abhängigkeit zur Kursversorgung.

Der Teilbereich Abwicklung verfügt im hier betrachteten Fallbeispiel ebenso über zwei zentrale Anwendungssysteme. Die Anbindung an die Daten aus dem Handel erfolgt jeweils direkt:

- Die Bestätigungen werden automatisch generiert (*Bestaetigung*). Hierbei ist es entscheidend, dass die Richtigkeit der Daten zeitnah sichergestellt wird. Die bestätigten Geschäfte fließen abschließend in die Bestandsführung ein.
- Die Bestandsführung in der Abwicklung erfolgt in einem separaten Anwendungssystem (*BackOffice*). Hieraus werden die anstehenden Zahlungen generiert und der Bestand auf Vollständigkeit und Richtigkeit hin überwacht.

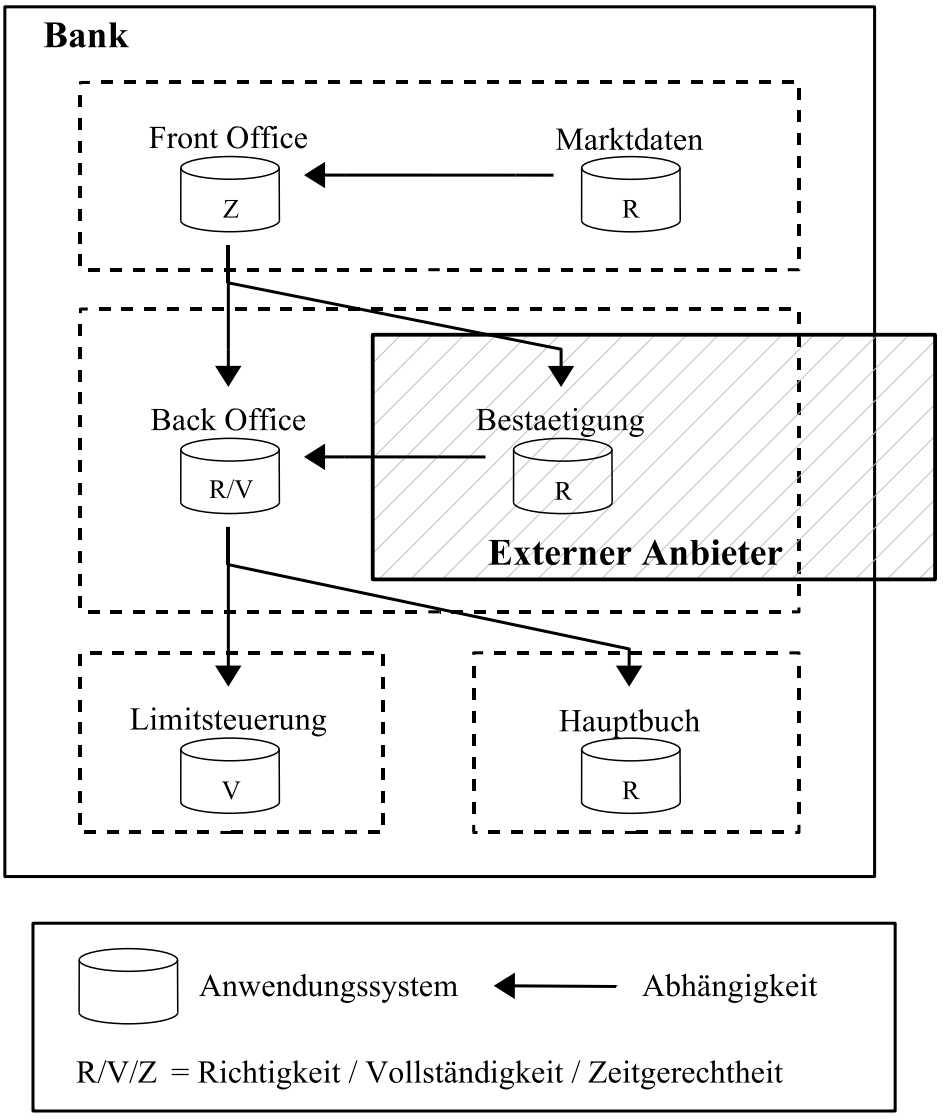

Abbildung 6.4: Systemlandschaft im Handelsprozess

Aus der Abwicklung werden die Transaktionen an das Risikocontrolling weitergeleitet, um die Geschäfte dort mittels unabhängiger Marktdaten zu prüfen:

- Besonders wichtig ist die Kontrolle auf Einhaltung der Limite (*Limitsteuerung*). Ferner sind alle Geschäfte zu bewerten und eine Gesamtrisikoposition zu ermitteln und zu melden.

Analog werden die Geschäfte von der Abwicklung auch an das Rechnungswesen übertragen, um in die Buchführung einzugehen:

- Das Hauptbuch (*Hauptbuch*) führt die buchhalterischen Bestände der Handelsgeschäfte, die in Abhängigkeit vom angewendeten Rechnungslegungsstandard bewertet werden. Ebenso ist dieses Anwendungssystem für die Ermittlung des externen Ergebnisses im Handel verantwortlich.

Aus der in Abbildung 6.4 dargestellten IT-Topologie wird eine Wissensbasis entsprechend der Technologierisiko-Ontologie aufgebaut. Die dargestellten direkten Abhängigkeiten sind gerichtet und stellen die in der Supportfunktion (vgl. Formel 4.12) enthaltenen Beziehungen zwischen den Anwendungssystemen dar. Über die in Kapitel 4.3 entwickelte Transformation wird die IT-Topologie als ein gerichteter Graph aus Assets interpretiert und auf das Simulationsmodell abgebildet.

Die schraffierte Fläche um das Anwendungssystem für die Bestätigungen verdeutlicht das Outsourcing Szenario. Der Vergleich der Geschäftsdaten mit denen des Kontrahenten ist nach einem Outsourcing nicht mehr in der Verantwortlichkeit der Bank und das Back Office von externen Daten abhängig.

6.3.2 Kritische Risikofaktoren

Als Auslöser möglicher Verluste werden die Einflüsse der IT-Komponenten und IT-Managementaufgaben untersucht. Die Ausprägungen der Risikofaktoren werden im Fallbeispiel über Bedrohungsszenarien abgeschätzt. Für die IT-Komponenten wird auf Bedrohungen entsprechend des IT-Grundschutzhandbuchs (siehe BSI ITGS) zurückgegriffen. Risiken aus Aufgaben des IT-Managements basieren im Wesentlichen auf dem COBIT Standard (siehe ITGI COBIT).

Die Bedrohungsszenarien sind mit den verursachenden Risikofaktoren und den betroffenen Anwendungssystemen sowie ihren Eigenschaften in Tabelle 6.3 dargestellt. Die Beschreibung der Bedrohung ist eng an den jeweiligen Standard angelehnt. Die letzte Spalte zeigt die Häufigkeit (Häufig, Gelegentlich, Selten), die für das jeweilige Ereignis im Fallbeispiel angenommen wird.

Beschreibung des Bedrohungsszenarios	**Verursachender Risikofaktor**	**Anwendungs-system**	# **H**	**G**	**S**
„Ausfall von Netzkomponenten“ Durch eine Störung der Reutersanbindung kommt es zu einem Verlust der Verfügbarkeit der Kursversorgung und nicht mehr aktuellen Kursen ... (BSI-G 4.31)	Reuters ↪ Verfuegbarkeit	Marktdaten ↪ Richtigkeit		■	
„Ausfall der Stromversorgung“ Trotz hoher Versorgungssicherheit kommt es immer wieder zu Unterbrechungen der Stromversorgung und damit zu Ausfällen des Handelssystems ... (BSI-G 4.1)	Stromversorgung ↪ Verfuegbarkeit	FrontOffice ↪ Zeitgerechtheit			■
„Unzureichende Datenbank-Sicherheit“ Falsche Einstellung der Sicherheitsmechanismen der Datenbank-Standardsoftware gefährden die Richtigkeit der darin gespeicherten Bestätigungen ... (BSI-G 2.38)	BestaetigungDB ↪ Vertraulichkeit	Bestaetigung ↪ Richtigkeit			■
„Managing facilities“ Schwächen im Management der für den IT-Betrieb genutzten Anlagen führen zu einer falschen Verarbeitung der Bestätigungen ... (COBIT-DS 12)	FacilityManagement ↪ Effektivitaet	Bestaetigung ↪ Richtigkeit	■		
„Ausfall der Datenbank“ Steht die Datenbank im Back Office, z.B. aufgrund von Hard- oder Software-Problemen, nicht zur Verfügung ist die Richtigkeit des Bestands nicht gewährleistet ... (BSI-G 4.26)	PortfolioDB ↪ Funktionstuechtigkeit	BackOffice ↪ Richtigkeit		■	
„Managing data“ Schwächen im Datenmanagement verursachen eine unvollständige Bearbeitung oder Speicherung der Datenbestände ... (COBIT-DS 11)	Datenmanagement ↪ Effektivitaet	BackOffice ↪ Vollstaendigkeit	■		
„Software-Schwachstellen“ In zu komplexer Standardsoftware treten Programmierfehler auf, die zu einer unvollständigen Verarbeitung führen ... (BSI-G 4.22)	BewertungSoftware ↪ Funktionstuechtigkeit	Limitsteuerung ↪ Vollstaendigkeit			■
„**Managing projects**“ Ein schlechtes Projektmanagement erhöht den Druck auf laufende Vorhaben und verursacht Fehler im Rechnungswesen ... (COBIT-PO 10)	Projektmanagement ↪ Effizienz	Hauptbuch ↪ Richtigkeit			■

Tabelle 6.4: Risikofaktoren IT-Komponenten / IT-Managementaufgaben

Gemäß bisheriger Studien sind die Häufigkeiten von technischen Verlustereignissen (wie Hardwarefehler) als eher gering einzustufen. Dagegen kommen prozessuale Fehler (wie Versagen des IT-Managements) häufiger vor.

Die qualitativ beschriebenen Häufigkeiten müssen vor der Simulation auf konkrete Werte für die durchschnittliche Anzahl jährlicher Ausfälle abgebildet werden. Die Bedrohungsszenarien sind im Simulationsmodell als Bernoulli-verteilte Input-Größen enthalten. Der angenommene Verteilungsparameter entspricht der Anzahl der Ausfälle pro Jahr geteilt durch 365 Tage.

Durch ein Outsourcing des Betriebs einzelner Anwendungssysteme können sich die Eintrittswahrscheinlichkeiten der Bedrohungsszenarien in Abhängigkeit von der Qualität des Dienstleisters erhöhen oder verringern.

6.3.3 Finanzielle Effekte

Die Höhe der finanziellen Effekte wird in der vorgeschlagenen Ontologie-zentrierten Vorgehensweise über unabhängige Verlustverteilungen modelliert. Dazu werden stochastische Ausgabegrößen im Umfeld der zentralen Anwendungssysteme beziehungsweise Aktivitäten definiert und daraus der gesamte Verlust als Summe aller Einzelverluste über ein Jahr ermittelt. Beim zu vergleichenden Standardansatz wird der Nettoertrag aus Finanzgeschäften als zentrale Größe zur Risikoquantifizierung verwendet. Daher wird bei der Abschätzung der Verlustverteilungen im Wesentlichen auch auf diese Größe zurückgegriffen. Folgend wird in drei Bereichen (Handel, Abwicklung, Rechnungswesen) des Handelsprozesses jeweils ein konkreter Schätzer für die Verlustpotentiale gesucht. Um das Fallbeispiel einfach zu halten, werden Verluste aus dem Risikocontrolling indirekt über den Handel abgebildet.

Fällt im Handelsprozess das zentrale Anwendungssystem Front Office Hard- oder Software-bedingt aus, ist der Umfang des (elektronischen) Handels stark eingeschränkt. Der Basler Ausschuss beschreibt den folgenden Aspekt als *„Business disruption and system failures.“* Das umfasst beispielsweise *„[...] hardware and software failures, telecommunication problems, and utility outages.“*(BCBS 2003b, S.2)

An solchen Tagen wird konsequenterweise aufgrund des gesunkenen Umsatzes auch der durchschnittliche Ertrag im gesamten Geschäftsfeld Handel nicht erreicht. Aus dieser Betrachtung werden jedoch extreme Verluste ausgenommen, die aufgrund der fehlenden Reaktionsmöglichkeit auf massive Marktbewegungen resultieren. Als Schätzer für das Risikopotential wird das durchschnittliche Handelsergebnis umgerechnet auf einen Handelstag angesetzt.

Ein weiteres Potential für wesentliche Verluste entsteht in der Abwicklung. Aufgrund der Zuständigkeit für sämtliche externe Zahlungen, ist die korrekte Verarbeitung aller Informationen hier besonders wichtig. So können falsche Transaktionen einen direkten finanziellen Verlust auslösen. Basel II beschreibt diesen Aspekt als *„losses from failed transaction processing or process management, from relations with trade counterparties and vendors."* (Basel II, Anhang 9)

Besonders die im Basler Anhang 9 genannten Beispiele „Fehlerhafte Lieferung" und „Überschreiten eines Termins oder Nichterfüllung einer Aufgabe" sind für den Teilbereich Abwicklung relevant. Entscheidende Größe für mögliche Verluste ist das tägliche Zahlungsvolumen (Ein- und Auszahlungen). Ergeben sich hier Fehler oder Verzögerungen, können Zinsausfälle sowie Strafen die Folge sein.

Im Rechnungswesen verursachen nicht sachgemäß geführte Bestände oder falsch ermittelte Ergebnisbeiträge eine Korrektur mit bilanzieller Auswirkung. Ähnlich wie in der Abwicklung können hierfür Fehler in der maschinellen Verarbeitung der Daten verantwortlich sein. Basel II nennt beispielhaft die Bedrohung *„Accounting error"* oder *„entity attribution error"* (Basel II, Anhang 9).

Entscheidende finanzielle Einflussgröße für das Rechnungswesen ist das handelsrechtliche Ergebnis sowie die bilanzwirksamen Bestandskonten. Um den Vergleich mit dem Standardansatz zu erleichtern, wird im Rahmen des Fallbeispiels das Handelsergebnis als Bezugsgröße gewählt.

Für die Modellierung der dargestellten Verluste wird in der Ontologie-zentrierten Simulation auf unterschiedliche Wahrscheinlichkeitsverteilungen zurückgegriffen. Wie in Kapitel 4.3.4 erläutert kommen besonders die Lognormal-, die Weibull oder die Gamma-Verteilung in Betracht. Um das Fallbeispiel nicht ausschließlich über eine einzige Verteilung zu analysieren, werden die drei Verteilungen innerhalb der Ontologie-zentrierten Simulation alternativ betrachtet. Um die Vergleichbarkeit zu gewährleisten, werden jeweils der Erwartungswert sowie die Standardabweichung normiert.

Das Outsourcing kann die Verlustverteilung verändern. Durch den Abschluss eines Service Level Agreements ist es möglich, im Fall eines Verlusts den Dienstleister in Regress zu nehmen und den finanziellen Schaden zu kompensieren. Diese Vorgehensweise entspricht der Berücksichtigung einer Versicherung (vgl. BCBS 2003a, S.18f.). Dabei ist einerseits immer die Ausgestaltung des Vertrags zu berücksichtigen. Andererseits kann eine Eigenkapitalbeteiligung am Dienstleister (z.B. Tochtergesellschaft) dazu führen, dass der Verlust mit eigenen Mitteln abgesichert und das Risiko so nur partiell reduziert wird.

6.3.4 Auswertung einer Simulation

Um die beiden Alternativen zur Risikoquantifizierung unter dem Einfluss der genannten Szenarien im Detail zu untersuchen, wird eine Simulation auf Basis eines vorgegebenen Zahlenwerks ausgewertet. Grundlage stellt das Geschäftsfeld Handel eines exemplarischen Kreditinstitutes dar, das der idealtypischen Struktur deutscher Großbanken entspricht. In der folgenden Tabelle 6.5 sind hierzu der jährliche Ergebnisbeitrag im Geschäftsfeld Handel, das jährliche Volumen der Ein- und Auszahlungen sowie das entsprechende Ergebnis im Rechnungswesen aufgeführt. Die erwarteten Zahlen stellen die Grundlage für das Simulationsmodell dar. Die Schwankung bezeichnet die mögliche Streuung der Werte um das erwartete Mittel und stellt daher ein Maß für die Genauigkeit der Schätzung der jeweiligen Größe dar. Im Rahmen des Fallbeispiels werden der Ergebnisbeitrag im Handel sowie das Ergebnis im Rechnungswesen vereinfachend aufeinander abgestimmt. Um jedoch dem andersartigen Charakter der beiden Größen Rechnung zu tragen, werden unterschiedliche Schwankungen unterstell

Größe	Erwartungswert	Schwankung
Ergebnisbeitrag im Handel	100 Mio. EUR	50 Mio. EUR
Volumen der Ein- und Auszahlungen	20 Mrd. EUR	5 Mrd. EUR
Ergebnis im Rechnungswesen	100 Mio. EUR	10 Mio. EUR

Tabelle 6.5: Mögliche Großbank

In den nächsten Absätzen wird die Umsetzung des in den Kapiteln 6.3.1 bis 6.3.3 vorgestellten Fallbeispiels in das Ontologie-zentrierte Simulationsmodell erläutert. Oben genannte Zahlen stellen hierbei den äußeren Rahmen dar. Das in den Formeln 4.12 und 4.13 entwickelte Modell funktionaler Abhängigkeiten wird auf die spezifischen Begebenheiten des Fallbeispiels angepasst (vgl. Formel 6.1). Um die identifizierten direkten Abhängigkeiten zwischen den Anwendungssystemen vollständig zu berücksichtigen, wird $\omega = 1$ gesetzt. Dadurch wirken sich Systemausfälle direkt auf nachgelagerte Anwendungssysteme aus. Die Zeitabhängigkeit wird auf den jeweils gleichen Handelstag t beschränkt, so dass $\alpha = 0$ gesetzt werden kann. Im Fallbeispiel wird davon ausgegangen, dass alle Zustandsveränderungen durch Anwendungssysteme oder Risikofaktoren festgelegt sind ($\xi = 0$). Die Störgröße ist daher in der Formel 6.1 nicht enthalten. Die Risikofaktoren beeinflussen den Zustand des Anwendungssystems direkt negativ, so dass β auf -1 gesetzt wird. Die ursprüngliche Unterstützung

wird mit $\vartheta = 1$ angenommen, so dass sich Zustandsveränderungen mindestens eines vorgelagerten Systems oder eines beeinflussenden Risikofaktors negativ auf den Zustand der Anwendungssysteme auswirken.

$$n_i^e(t) = \Theta\left(-\left(1 - \sum_{\substack{Asset\ j \\ State\ s \in j}} n_j^s(t) + \sum_{\substack{Riskfactor\ k \\ State\ u \in k}} -Y_k^u(t)\right)\right) \tag{6.1}$$

Die hier festgelegten Parameter gelten ausschließlich für das Fallbeispiel. Sie beinhalten keine Aussagen über allgemeingültige Zusammenhänge für die im Rahmen dieser Arbeit vorgestellte Vorgehensweise.

Für die Umsetzung der Risikofaktoren müssen die in Tabelle 6.4 qualitativ beschriebenen Häufigkeiten in quantitative Größen überführt werden. Dazu werden zwei Szenarien gebildet. Das erste Szenario (normale Fehlerhäufigkeit) unterstellt durchschnittliche Fehlerhäufigkeiten, in denen zum Beispiel Gegenmaßnahmen teilweise bereits berücksichtigt sind. Im zweiten Szenario wird ein weniger effektives IT-Management unterstellt, so dass die Häufigkeiten von Fehlern in der Regel oberhalb des ersten Szenarios liegen:

- normale Fehlerhäufigkeit: H=5, G=3, S=1 (Anzahl pro Jahr)
- erhöhte Fehlerhäufigkeit: H=8, G=5, S=1 (Anzahl pro Jahr)

Die täglichen finanziellen Effekte ergeben sich aus den in Tabelle 6.5 dargestellten Daten. Als tägliches Verlustpotential im Handel wird direkt das anteilige (1/365) jährliche Handelsergebnis verwendet. In der Abwicklung wird das anteilige (1/365) jährliche Zahlungsvolumen der Ein- und Auszahlungen als Basis angenommen. Der finanzielle Effekt ergibt sich hier in Form eines Zinsverlustes, hier exemplarisch zu einem Zins von 5% gerechnet auf 10 Tage. Für das Rechnungswesen ist ebenso wie im Handel das tägliche anteilige Ergebnis relevant, jedoch hier nur indirekt. Der Wert wird zusätzlich mittels eines Fehlerpotentials adjustiert, hier beispielsweise 10%.

Da in der Abwicklung das Outsourcing vorgenommen wird, werden hier unterschiedliche Szenarien betrachtet. Die Sourcing-Strategie kann als eine Auslagerung an einen Dienstleister mit oder ohne Eigenkapitalbeteiligung sowie als Insourcing betrieben werden. Für das Fallbeispiel wird das Verlustpotential voll, anteilig oder gar nicht, jeweils entsprechend der Absicherung durch Service Level Agreements, berücksichtigt:

- Outsourcing ohne Eigenkapital: 0% Verlustpotential der Abwicklung
- Outsourcing mit Eigenkapital: 50% Verlustpotential der Abwicklung
- kein Outsourcing: 100% Verlustpotential der Abwicklung

Der gesamte Verlust ergibt sich entsprechend Formel 4.32 als stochastischer Prozess über die einzelnen Verluste:

$$L(T=365)=\sum_{t=1}^{T}(L_{Handel}(t)+L_{Abwicklung}(t)+L_{Rechnungswesen}(t)) \tag{6.2}$$

Wie in Kapitel 4.3.5 beschrieben, erfolgt die Ermittlung der Gesamtverlustverteilung mittels einer Simulation. Abbildung 6.5 zeigt exemplarisch den Verlauf des VaR eines simulierten Szenarios. Der VaR zeigt im betrachteten Szenario ein leicht oszillierendes Konvergenzverhalten. Um belastbare Ergebnisse zu erzielen, wurde die Simulation für sämtliche Szenarien mit 200.000 Iterationen durchgeführt.

Im Rahmen des Fallbeispiels wird nun die Auswirkung der Szenarien auf die unterschiedlichen Alternativen zur Risikoquantifizierung untersucht. Als Alternativen werden hier allgemein die Ontologie-zentrierte Simulation und der Standardansatz gegenübergestellt. Um die Belastbarkeit der Szenarioanalyse weiter zu erhöhen, werden die Alternativen noch genauer variiert. Bei der Ontologie-zentrierten Simulation wird die Auswirkung unterschiedlicher Annahmen über die Verlustverteilung, hier die Lognormal-Verteilung, Weibull-Verteilung und Gamma-Verteilung (vgl. Kapitel 4.3.4), dargestellt. Auch für den Stan-

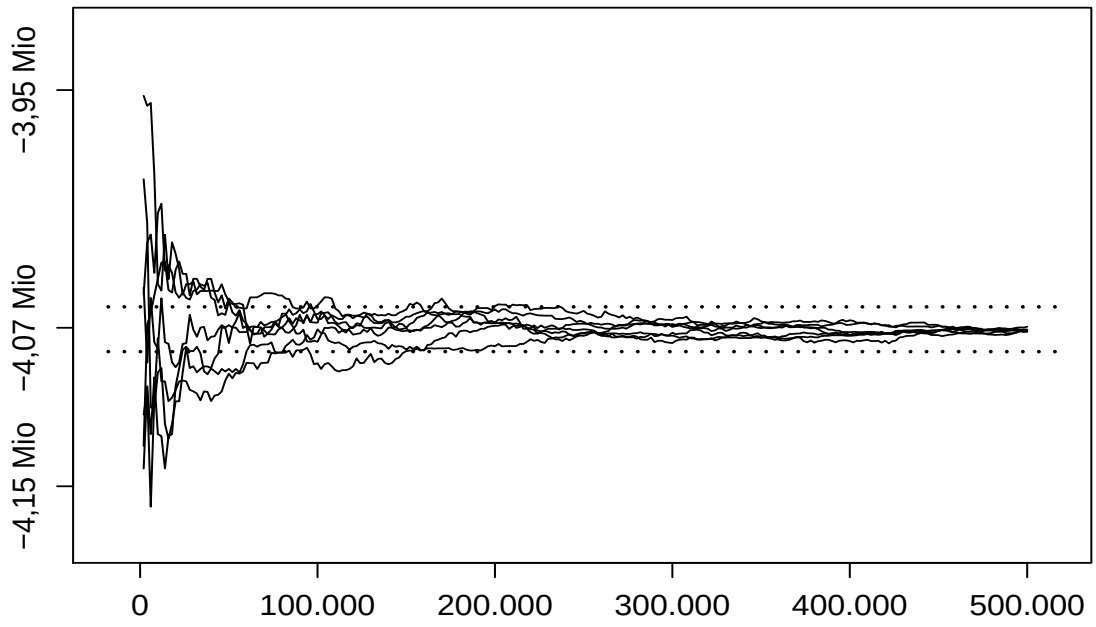

Abbildung 6.5: Konvergenz $VaR_{99,9}$
(Unterschiedliche Pfade eines exemplarischen Szenarios:
Mit Outsourcing, erhöhte Fehlerhäufigkeit)

dardansatz wird der Einfluss verschiedener Varianten untersucht. Hier wird die Auswirkung des angenommenen Anteils der Technologierisiken an den gesamten operationellen Risiken im Geschäftsfeld Handel (vgl. Tabelle 6.3)analysiert. Die Gegenüberstellung der Alternativen vor dem Hintergrund der unterschiedlichen Szenarien ist in Tabelle 6.6 zusammengefasst.

	Alternativen zur Quantifizierung					
	Ontologie-zentriert			**Standardansatz**		
Szenarien	**~ Lognormal**	**~Gamma**	**~Weibull**	**25%**	**30%**	**60%**
Ohne Outsourcing		❶			❷	
normale Fehlerhäufigkeit	*VaR:* 3,5 *CVaR:* 3,8	*VaR:* 3,2 *CVaR:* 3,5	*VaR:* 3,1 *CVaR:* 3,4	4,5	5,4	10,8
erhöhte Fehlerhäufigkeit	*VaR:* 4,7 *CVaR:* 5,1	*VaR:* 4,2 *CVaR:* 4,5	*VaR:* 4,1 *CVaR:* 4,5	4,5	5,4	10,8
Outsourcing mit EK	❸					
normale Fehlerhäufigkeit	*VaR:* 3.3 *CVaR:* 3,6	*VaR:* 3,1 *CVaR:* 3,4	*VaR:* 3,0 *CVaR:* 3,4	4,5	5,4	10,8
erhöhte Fehlerhäufigkeit	*VaR:* 4,4 *CVaR:* 4,7	*VaR:* 4,1 *CVaR:* 4,4	*VaR:* 4,1 *CVaR:* 4,4	4,5	5,4	10,8
Outsourcing ohne EK						
normale Fehlerhäufigkeit	*VaR:* 3,1 *CVaR:* 3,4	*VaR:* 3,0 *CVaR:* 3,4	*VaR:* 3,0 *CVaR:* 3,3	4,5	5,4	10,8
erhöhte Fehlerhäufigkeit	*VaR:* 4,1 *CVaR:* 4,4	*VaR:* 4,1 *CVaR:* 4,3	*VaR:* 4,0 *CVaR:* 4,4	4,5	5,4	10,8

Tabelle 6.6: Ergebnisse Simulation / Standardansatz
(Alle Angaben in Mio. EUR)

Betrachtet man die unterschiedlichen Verteilungen, verschiebt sich das durch das Risikomaß ermittelte Risikopotential (❶) entsprechend Abbildung 4.1. Das kann mit dem unterschiedlichen Verhalten im Rand der Verteilung begründet werden. Der CVaR liegt natürlicherweise immer über dem VaR. Die möglichen Prozentsätze im Standardansatz zeigen die große Spannweite in der Höhe des Risikopotentials (❷). Je nachdem, wie die unterschiedlichen Verlustdatensammlungen interpretiert werden, können Risikopotentiale zwischen 4,5 und 10,8 Mio. EUR ermittelt werden. Vergleicht man nun die unterschiedlichen Szenarien der Sourcing-Strategie, nimmt das Risikopotential unabhängig von der gewählten Verteilung in Abhängigkeit vom Grad des Outsourcings ab (❸).

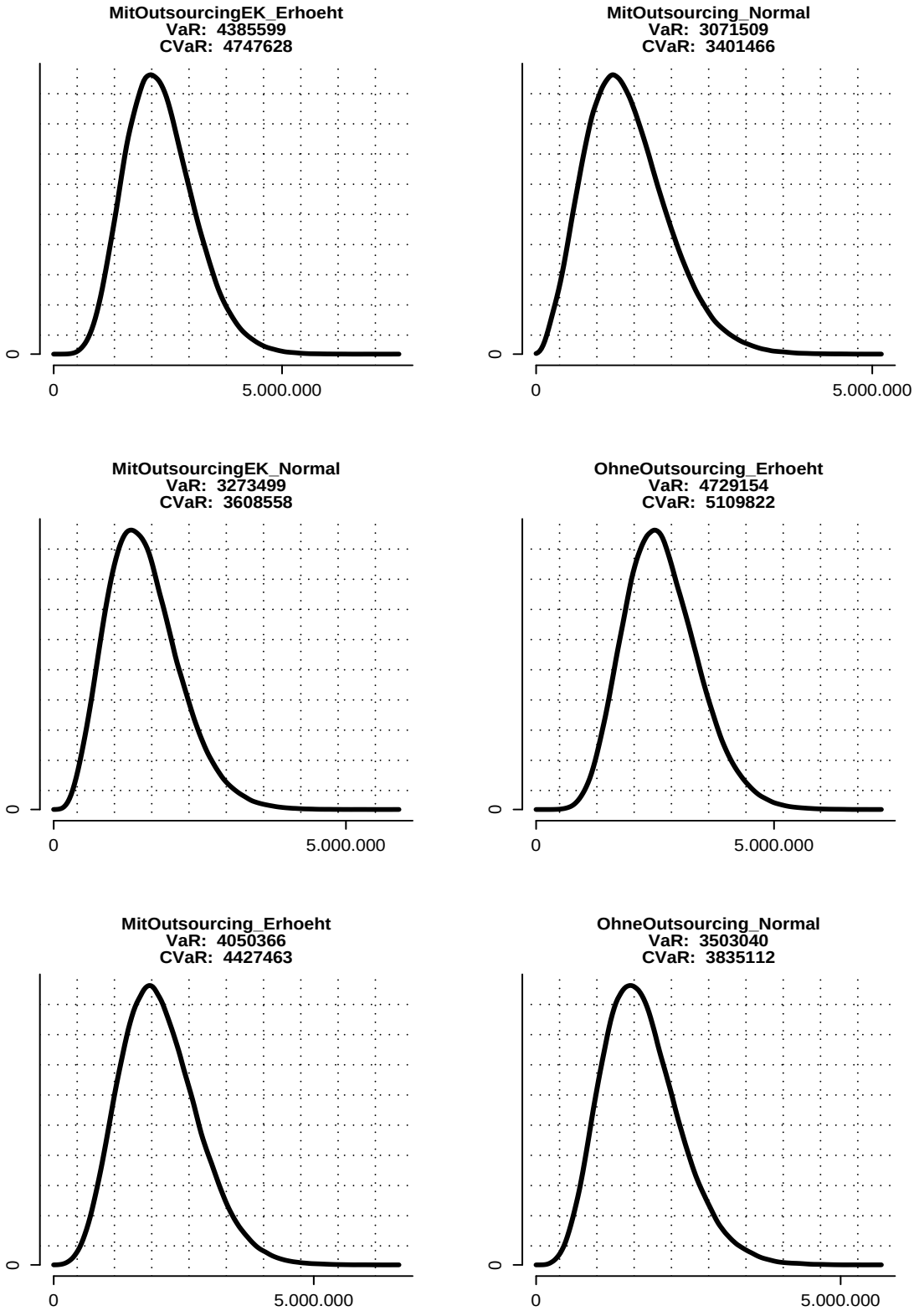

Abbildung 6.6: Verlustverteilung der Szenarien
(Exemplarisch für die Lognormal-Verteilung)

Hierbei bleibt das Verhältnis zwischen einer normalen und einer erhöhten Fehlerhäufigkeit über die Strategien hinweg erhalten. Zusammenfassend kann festgehalten werden, dass das mit dem Standardansatz ermittelte Risikopotential unabhängig von der gewählten Sourcing-Strategie ist, wohingegen die Ontologie-zentrierte Simulation auf die veränderte Risikosituation sensitiv reagiert. Die Abbildung 6.6 zeigt die der Tabelle 6.6 zugrunde liegenden Verlustverteilungen.

6.3.5 Einordnung der Ergebnisse

Die entscheidende Fragestellung im Rahmen dieser Arbeit ist die direkte Auswirkung der Methode zur Quantifizierung auf das Risikomanagement der Bank. Hier muss sowohl die regulatorische als auch die bankinterne Sichtweise berücksichtigt werden.

Für den ersten Punkt ist besonders der Einfluss der Quantifizierungsmethode auf das vorzuhaltende regulatorische Kapital relevant. Es ist davon auszugehen, dass die Kapitalanforderung mit steigender Fortschrittlichkeit der Methode zur Quantifizierung reduziert werden kann. Aufgrund des nicht unerheblichen Anteils der operationellen Risiken am gesamten ökonomischen Kapital (vgl. Tabelle 6.7) scheint der Einsatz genauerer Methoden sinnvoll.

Risikobericht 2004 (im Konzern)	**Operationelle Risiken**		**Anteil an Gesamt**		**Ansatz**
	2004	**2003**	**2004**	**2003**	
Commerzbank 2004	1.300	900	13%	9%	AMA
Deutsche Bank 2004	2.243	2.282	17%	15%	AMA
Dresdner Bank 2004	1.100	1.100	11%	10%	AMA
Hypovereinsbank 2004	1.206	1.364	15%	14%	AMA
Postbank 2004	*k.A.*	*k.A.*	*k.A.*	*k.A.*	*AMA*

Tabelle 6.7: Ökonomisches Kapital deutscher Großbanken
(Spalte 2 und 3 in Mio. EUR, Gesamt (Risikopotential*12,5) vor Diversifikation)

Im vorliegenden Fallbeispiel kann zur direkten Auswirkung auf das regulatorische Kapital trotz des Zahlenverhältnisses in Tabelle 6.6 keine absolute Aussage getroffen werden. Es wäre hierzu ein konkreter Vergleich der Ontologie-zentrierten Simulation mit den jeweils verwendeten Ansätzen unter institutsspezifischen Annahmen notwendig.

Für die bankinterne Sicht ist es jedoch entscheidend, dass die vorgeschlagene Ontologie-zentrierte Simulation die Risikosituation ursächlicher abbildet als der Standardansatz. Insbesondere im Hinblick auf Outsourcing ist ein höherer Detaillierungsgrad auch im Sinne der Bundesbank wichtig: *„Die operationellen Risiken (z.B. Rechtsrisiken) aus solchen Auslagerungen, die als Verlust auf das Institut durchschlagen können, sind im AMA und bei der Risikosteuerung zu berücksichtigen.“* (Deutsche Bundesbank und BaFin 2005, S.24)

Gerade bei den in Tabelle 6.7 genannten Kreditinstituten wird zur Quantifizierung der operationellen Risiken nicht ausschließlich der Standardansatz verwendet. Obwohl die Risikosituation im dargestellten Outsourcing-Fallbeispiel durch den Einsatz von Self-Assessments und Risikoindikatoren ursächlicher ermittelt werden könnte (vgl. Deutsche Bundesbank und BaFin 2005, S.24), bleiben die in Kapitel 4.2.4 dargestellten Schwächen der fortgeschrittene Messansätze gegenüber der Ontologie-zentrierten Simulation bestehen.

6.4 Zusammenfassung

Ein Ziel der Darstellung des Fallbeispiels war es, die prinzipielle Anwendbarkeit der Ontologie-zentrierten Simulation zu demonstrieren und ihre Vor- und Nachteile zu verdeutlichen. Die Diskussion unterschiedlicher Aspekte, wie der Beschreibung einer Systemlandschaft, der Identifikation möglicher Risiken und der Ableitung potentieller Verluste, zeigt die grundsätzliche Anwendbarkeit der Vorgehensweise.

Besonders mit Blick auf das bankinterne Management der Technologierisiken wird der Vorteil der Ontologie-zentrierten Simulation sehr deutlich. Betrachtet man das erste zentrale Ziel dieser Arbeit (vgl. Kapitel 1.2, Ziele 1a - 1c), wird die Unterstützung einer risikobezogenen IT-Governance erkennbar:

- Durch die Verwendung der Technologierisiko-Ontologie wird der Basler Risikobegriff um wesentliche Konzepte der IT-Governance, wie beispielsweise COBIT oder IT-Grundschutz, erweitert. Darüberhinaus ist das verwendete Risikoverständnis nicht nur intern bekannt, sondern wird durch die Ontologie explizit und nachvollziehbar dargestellt.
- Existierende Strukturen und Zusammenhänge sind im Risikomodell und damit im ermittelten Risikopotential enthalten.
- Strukturelle Veränderungen, wie im Fallbeispiel durch das Outsourcing, werden explizit dargestellt und in der Risikobetrachtung berücksichtigt.

Betrachtet man das zweite zentrale Ziel (vgl. Kapitel 1.2, Ziele 2a + 2b) zeigt sich der Vorteil der Ontologie-zentrierten Simulation insbesondere im Hinblick auf eine ursachengerechte Risikoabbildung:

- Die Objektivität des ermittelten finanziellen Risikopotentials ist aufgrund unterschiedlicher Annahmen im Simulationsmodell (z.B. Verteilungen) zwar nur eingeschränkt nachweisbar, dafür sind die getroffenen Annahmen explizit und können mit empirischen Daten (wie z.B. der LDCE oder interne Schadensdatenbanken) abgeglichen werden.
- Die Risikosensitivität ist deutlich höher als bei der Anwendung eines Standardansatzes oder der Verwendung einer Schadensdatenbank. Das Risikopotential aus dem Einsatz der Informationstechnologie lässt sich sachgemäß abbilden.

Durch die Anwendung der Ontologie-zentrierten Vorgehensweise im Kontext des Fallbeispiels kann die Argumentation aus Kapitel 4.4 weitergeführt werden. Es werden nicht nur die untersuchten Kriterien Verständnis und Quantifizierung erfüllt, vielmehr kann auch die Vorteilhaftigkeit im Sinne eines effizienten Risikomanagements begründet werden. Das Fallbeispiel verdeutlicht auch, dass die Umsetzung in einer konkreten Bank mit höheren Kosten verbunden sein dürfte. Die konkrete Entscheidung für eine der Vorgehensweisen wird sicherlich unter Berücksichtigung der Risikosituation des zu untersuchenden Geschäftsfeldes und der Größe der Bank zu treffen sein.

Kapitel 7
Abschließende Betrachtung

Das eigentliche Ziel dieser Arbeit war die Entwicklung einer Vorgehensweise zur Quantifizierung operationeller Technologierisiken, um hierüber eine Entscheidungsunterstützung im Risikomanagement bei Kreditinstituten zu liefern. Dem Bankmanagement soll dadurch ein weiteres Werkzeug zur Verfügung gestellt werden, auf die gestiegene Bedeutung der Informationstechnologie auch durch ein geeignetes quantitatives Risikomanagement reagieren zu können. Im Kontext der Wirtschaftsinformatik lässt sich dieser Anspruch abstrakt als Verbindung zweier Teilziele beschreiben (vgl. Becker et al. 2004, S.346ff.): Die Erlangung modelltheoretischer sowie methodischer Erkenntnisse in einem konkreten betriebswirtschaftlichen Anwendungsbereich, hier dem Technologierisiko-Management bei Kreditinstituten. Entsprechend dieser Zielsetzung wurde der Forschungsansatz für diese Arbeit gewählt. Zunächst stand die Entwicklung eines normativen Modells im Vordergrund, welches ein Verständnis dieser in Teilen noch unscharfen Risikokategorie aus unterschiedlichen Perspektiven erlaubt. Auf dieser Grundlage wurde eine Methode zur Quantifizierung operationeller Technologierisiken vorgeschlagen, die das inhaltliche und das quantitative Verständnis integriert. Abschließend wurde die entwickelte Vorgehensweise über die Implementierung eines Prototyps unter technischen Gesichtspunkten überprüft sowie über die Analyse eines anwendungsbezogenen Fallbeispiels fachlich evaluiert. Die zentralen Ergebnisse der vorliegenden Arbeit werden nun im Folgenden noch einmal kritisch gewürdigt und ein Ausblick über weitere Entwicklungsmöglichkeiten gegeben.

7.1 Ergebnisse

Ausgangslage für diese Arbeit war die hohe Bedeutung von Informationstechnologie für Kreditinstitute sowie die damit einhergehende Notwendigkeit, die resultierenden Technologierisiken in ein bankweites Risikomanagement zu integrieren. Hier bewegt sich das Risikomanagement jedoch stets in einem Spannungsfeld zwischen interner und regulatorischer Sicht. Auf der einen Seite be-

greifen Banken das Management ihrer Technologierisiken als Teil einer IT-Governance. Hierbei stellt die ursachengerechte Quantifizierung der Risiken eine wichtige Voraussetzung dar, um geeignete Steuerungs- oder Verbesserungsmaßnahmen durchführen zu können. Auf der anderen Seite berücksichtigen auch die deutsche beziehungsweise die europäische Bankenregulierung die operationellen Technologierisiken und machen hierzu konkrete qualitative und quantitative Vorgaben für das Risikomanagement. Die in Basel II vorgeschlagenen Ansätze zur Quantifizierung stehen primär im Zeichen einer Maximierung der Ausfallsicherheit; die unternehmerische Sicht ist hier eher zweitrangig. Hieraus ergibt sich ein Spannungsfeld zwischen dem bankinternen Streben nach Optimierung der Risikokapitalkosten und dem regulatorischen Anspruch höchstmöglicher Sicherheit im Bankensektor.

Die bisher in der Literatur existierenden Ansätze zur Quantifizierung nehmen in der Regel entweder nur die interne oder die externe Sicht ein und berücksichtigen das genannte Spannungsfeld somit nicht ausreichend. Aus diesem Grund wurde die Entwicklung einer neuen Vorgehensweise zur ursächlichen Risikoquantifizierung unter Erfüllung regulatorischer Anforderungen als Ziel dieser Arbeit formuliert. Die zur Umsetzung dieser Vorgehensweise verwendeten Forschungsmethoden werden nun anhand der einzelnen Teilaspekte Modellbildung, Methodenentwicklung, prototypische Implementierung und Evaluation mittels Fallbeispiel einer kritischen Würdigung unterzogen.

In einem ersten Schritt liefert die Bildung eines normativen **Modells** operationeller Technologierisiken bei Kreditinstituten einen wichtigen Beitrag zum Verständnis dieser Risikokategorie. Durch die direkte Betrachtung des IT-Umfelds der Bank können die technologischen Risikoursachen in Bezug zu einem allgemeinen Risikoverständnis gesetzt werden. Ferner verbindet das Modell durch die Einbindung akzeptierter IT-Standards die bankinterne mit der regulatorischen Sichtweise. Dies gewährleistet zudem indirekt einen hohen Grad an Akzeptanz, da das inhärente Risikoverständnis allgemeinen Normen folgt. Das vorgeschlagene Modell zielt letztendlich darauf ab, auf Basis der wissenschaftlichen Literatur sowie der relevanten IT-Standards ein akzeptiertes Verständnis operationeller Technologierisiken zu schaffen. Das im Rahmen dieser Arbeit beschriebene Modell ist jedoch nicht als abgeschlossen anzusehen. Beispielsweise ist keine explizite Abgrenzung der Technologierisiken von Markt- oder Kreditrisiken auf Ebene einzelner Verlustereignisse möglich. Derartige Erweiterungen oder Einschränkungen sind aber aufgrund der Repräsentation des Modells als formale Ontologie leicht und nachvollziehbar möglich. Des Weiteren bleibt noch anzumerken, dass für die Verwendung formaler Ontologien zur Modellierung in der praktischen Umsetzung bislang eher eingeschränkt Erfahrung vorhanden ist.

Aufbauend auf dem normativen Modell muss die Vorgehensweise zur Entscheidungsunterstützung um eine geeignete **Methode** der Risikoquantifizierung ergänzt werden. Ähnlich wie bei der Entwicklung des Modells werden hier regulatorische und interne Anforderungen berücksichtigt. Im Sinne der Terminologie von Basel II kann die Methode als Bestandteil eines fortgeschrittenen Messansatzes klassifiziert werden. Kerngedanke ist es, ein auf funktionalen Zusammenhängen basierendes Modell mit dem oben beschriebenen fachlichen Modell operationeller Technologierisiken zu verknüpfen. Über die automatische Erzeugung eines Simulationsmodells kann aus dem Risikoverständnis auch das finanzielle Risikopotential eines Kreditinstitutes ursachengerecht ermittelt werden. Da zur Entscheidungsunterstützung hier im Wesentlichen auf eine Simulation zurückgegriffen wird, sind die Ergebnisse zwangsläufig von der Wahl der Simulationsparameter abhängig. Hier soll daher noch einmal darauf hingewiesen werden, dass ein kontinuierliches Backtesting notwendiger Bestandteil einer solchen Vorgehensweise sein muss. Ferner ist die Güte der Ergebnisse ebenso vom Detaillierungsgrad des zugrundeliegenden Modells der IT-Umgebung abhängig. Hier sind die durch eine genauere Methode realisierten Vorteile in der Kapitalallokation jedoch stets ins Verhältnis zum verursachten Mehraufwand durch eine detailliertere Modellierung zu setzen und kritisch zu beurteilen.

In einem letzten Schritt muss die technische Machbarkeit sowie die fachliche Anwendbarkeit untersucht werden. Dazu wurde zuerst auf den Forschungsansatz der Entwicklung eines **Prototyps** zurückgegriffen und die entscheidenden Aspekte der vorgeschlagenen Vorgehensweise einer Ontologie-zentrierten Simulation implementiert. Auf dieser Grundlage erfolgte in einem letzten Schritt die Evaluation der Vorgehensweise über ein **Fallbeispiel**. In diesem wurde die vorgeschlagene Methode zur Risikoquantifizierung über die Analyse unterschiedlicher Szenarien in einem konkreten Geschäftsfeld kritisch untersucht. Obwohl das Fallbeispiel ausschließlich eine idealtypische deutsche Großbank betrachtet, liefert es zumindest im Rahmen des untersuchten Anwendungsfalls auch den fachlichen „proof of concept“.

7.2 Ausblick

Die in dieser Arbeit vorgeschlagene Vorgehensweise bezieht sich zwangsläufig auf einen speziellen Ausschnitt des unternehmensweiten Risikomanagements. An dieser Stelle ist daher eine mögliche Ausweitung auf andere Anwendungsfelder und Fachdomänen zu diskutieren. Ergänzend ist auch zu überlegen, inwieweit das Modell oder die Implementierung mit anderen aktuellen Ansätzen aus der Wirtschaftsinformatik in Verbindung gebracht werden kann.

Die Modellierung von Unternehmen und deren Strukturen, stellt in der Wirtschaftsinformatik ein aktuelles und wichtiges Thema dar (siehe Mobis 2006). Bedingt durch die Zielsetzung dieser Arbeit beschreibt das in Kapitel 3 vorgeschlagene Modell jedoch ausschließlich technologische Zusammenhänge unter Risikoaspekten. Basierend auf der Idee, gesamte Unternehmen mittels formaler Ontologien zu modellieren (siehe Uschold et al. 1998), könnten zusätzliche Aspekte in das Modell integriert werden. So wäre es denkbar, über das rein quantitative Verständnis hinaus, andere Elemente der Unternehmenssteuerung mit dem Risikomanagement zu verbinden. Ein mögliches Beispiel stellt die personelle Zuweisung von Verantwortlichkeiten für technologische Ressourcen dar. Alternativ könnten über die Anreicherung des Modells mit zusätzlichen Informationen auch weitere Risikokategorien operationeller Risiken nach Basel II wie Prozess- oder Humanrisiken in die Vorgehensweise integriert werden.

Eine Erweiterung in eine gänzlich andere Richtung stellt die folgende Überlegung dar. Der Einsatz von Techniken des Wissensmanagements, hier insbesondere die Wissensrepräsentation, sind innerhalb des Risikomanagementprozesses nicht auf die Phase der Quantifizierung beschränkt. Sie könnten vor allem auch während der Phase der Identifikation oder der Steuerung zum Einsatz kommen. Hier sind die Begleitung von Self-Assessments durch Ontologie-basierte Fragebögen oder die Entscheidungsunterstützung durch Expertensysteme vorstellbar (siehe Cuske et al. 2007).

Sämtliche im Rahmen dieser Arbeit angestellten Überlegungen beziehen sich auf Informationstechnologie und die damit verbundenen Risiken bei Kreditinstituten. Aber auch beispielsweise die Versicherungswirtschaft sieht sich mit dieser Herausforderung konfrontiert. Auch hier hat die Informationstechnologie einen ebenso starken Einfluss auf die Geschäftsprozesse, so dass das Management von Technologierisiken zu einem wesentlichen Bestandteil des holistischen Risikomanagements wird. Dieser Begebenheit trägt auch die durch das Lamfalussy-Verfahren initiierte Konsolidierung der europäischen Versicherungsaufsicht Rechnung. Ein wichtiger Bestandteil ist eine weitreichende Reform der Solvabilitätsrichtlinien (Solvency II). Hiermit berücksichtigt die Regulierung ab voraussichtlich 2010 auch für Versicherungsunternehmen erstmalig operationelle Risiken (siehe CEIOPS 2006). Entsprechend könnte die im Rahmen dieser Arbeit entwickelte Vorgehensweise grundsätzlich auch für Versicherungsunternehmen relevant sein.

Risikomanagement stellt zusammengefasst für alle Finanzdienstleistungsunternehmen eine entscheidende Kernkompetenz dar. In diesem Sinne kann davon ausgegangen werden, dass die hierfür verwendeten Methoden einem kontinuierlichen Weiterentwicklungsprozess unterliegen. Sicherlich ist ein nicht unerheblicher Anteil der aktuellen Dynamik der Einführung von Basel II im Bereich

von Kreditinstituten zuzuschreiben. Die Frage jedoch, inwieweit langfristig eine strenge Regulierung in Form von konkreten Vorschriften die inhaltliche Ausprägung beeinflussen soll, ist kritisch zu diskutieren. In diesem Kontext ist auch die Erläuterung zur Einführung der MaRisk (siehe BaFin 2005b) zu verstehen, die eine Abkehr von der traditionell regelbasierten hin zu einer prinzipienorientierten Aufsicht propagiert und damit einen Paradigmenwechsel einläutet. In solch einem Prozess kann gerade die Verwendung offener Verfahren, die auf akzeptierten Standards fußen und gleichzeitig unternehmerische Perspektiven nachvollziehbar integrieren, einen entscheidenden Beitrag leisten.

Anhang I
Technologierisiko-Ontologie

```
Namespace(xsd = <http://www.w3.org/2001/XMLSchema#>)
Namespace(rdf = <http://www.w3.org/1999/02/22-rdf-syntax-ns#>)
Namespace(rdfs = <http://www.w3.org/2000/01/rdf-schema#>)
Namespace(owl = <http://www.w3.org/2002/07/owl#>)

Ontology(http://www.jontorisk.org/trm.owl)


/**************************************************************
 * Object Properties
 **************************************************************/


ObjectProperty(compose domain(ValueChain)
                       range(Activity))

ObjectProperty(depend domain(ApplicationSystem)
                      range(ApplicationSystem))

ObjectProperty(determine domain(Effect)
                         range(Information))

ObjectProperty(exhibit domain(Ressource)
                       range(Property))

ObjectProperty(form domain(ITComponent)
                    range(ApplicationSystem))

ObjectProperty(generate domain(unionOf(Activity ExternalEvent))
                        range(Effect))

ObjectProperty(influence domain(ITManagementTask)
                         range(ApplicationSystem))

ObjectProperty(map domain(unionOf(Activity Property))
                   range(unionOf(BusinessLine EventType)))
```

```
ObjectProperty(operate domain(Ressource)
                       range(Activity))

ObjectProperty(operatedBy inverseOf(operate)
                       domain(Activity)
                       range(Resource))


/////////////////////////////////////////////////////////////
 * Classes
 /////////////////////////////////////////////////////////////


Class(Activity owl:Thing)

Class(ApplicationSystem partial Technology
              restriction(exhibit allValuesFrom(Compliance)))
DisjointClasses(ApplicationSystem ITComponent ITManagementTask)

Class(Availability partial Security)
DisjointClasses(Availability Integrity Confidentiality)

Class(BusinessLine complete oneOf(corporateFinance
                                  tradingSales
                                  retailBanking
                                  commercialBanking
                                  paymentSettlement
                                  agencyService
                                  assetManagement
                                  retailBrokerage))
SubClassOf(BusinessLine owl:Thing)

Class(BusinessRisk complete Loss restriction
                  (determine value(probability)))

Class(Completeness partial Compliance)
DisjointClasses(Completeness Correctness Timeliness)

Class(Compliance partial Property)
DisjointClasses(Compliance Security Soundness)

Class(Confidentiality partial Security)
DisjointClasses(Confidentiality Availability Integrity)

Class(Correctness partial Compliance)
DisjointClasses(Correctness Timeliness Completeness)

Class(CreditRisk partial BusinessRisk)
DisjointClasses(CreditRisk OperationalRisk)
```

```
Class(Introduction partial ITManagementTask)
DisjointClasses(Introduction Development Migration Operation
                Termination)

Class(Development partial ITManagementTask)
DisjointClasses(Development Termination Introduction Migration
                Operation)

Class(Effect partial owl:Thing)

Class(Effektiveness partial Soundness)
DisjointClasses(Effektiveness Efficiency Schedule)

Class(Efficiency partial Soundness)
DisjointClasses(Efficiency Schedule Effektiveness)

Class(Information complete oneOf(certainty probability uncertainty))
SubClassOf(Information owl:Thing)

Class(EventType complete oneOf(internalFraud
                               externalFraud
                               employmentPracticesWorplaceSafety
                               clientProductsBusinessPractices
                               damagePhysicalAssets
                               businessDisruptionSystemFailures
                               executionDeliveryProcessManagement))
SubClassOf(EventType owl:Thing)

Class(Expense partial Loss)
DisjointClasses(Expense Payment MissedGain)

Class(ExternalEvent partial owl:Thing)

Class(Gain partial Effect)
DisjointClasses(Gain Loss)

Class(Hardware partial ITComponent)
DisjointClasses(Hardware Infrastructure Software Network)

Class(Human partial Ressource)
DisjointClasses(Human Technology Process)

Class(Infrastructure partial ITComponent)
DisjointClasses(Infrastructure Software Hardware Network)

Class(Integrity partial Security)
DisjointClasses(Integrity Confidentiality Availability)

Class(InterestRateRisk partial BusinessRisk)
DisjointClasses(InterestRateRisk OperationalRisk)
```

```
Class(ITComponent partial Technology
                  restriction(exhibit allValuesFrom(Security)))
DisjointClasses(ITComponent ITManagementTask ApplicationSystem)

Class(ITManagementTask partial Technology
                 restriction(exhibit allValuesFrom(Soundness)))
DisjointClasses(ITManagementTask ITComponent ApplicationSystem)

Class(Loss partial Effect)
DisjointClasses(Loss Gain)

Class(MarketRisk partial BusinessRisk)
DisjointClasses(MarketRisk OperationalRisk)

Class(Migration partial ITManagementTask)
DisjointClasses(Migration Operation Development Termination
                Introduction)

Class(MissedGain partial Loss)
DisjointClasses(MissedGain Expense Payment)

Class(Network partial ITComponent)
DisjointClasses(Network Infrastructure Software Hardware)

Class(Operation partial ITManagementTask)
DisjointClasses(Operation Introduction Migration Termination
                Development)

Class(OperationalRisk complete BusinessRisk
              restriction(operatedBy allValuesFrom(Ressource)))
DisjointClasses(OperationalRisk CreditRisk ReputationRisk
                InterestRateRisk MarketRisk StrategyRisk)

Class(Payment partial Loss)
DisjointClasses(Payment MissedGain Expense)

Class(Process partial Ressource)
DisjointClasses(Process Human Technology)

Class(Property partial owl:Thing)

Class(ReputationRisk partial BusinessRisk)
DisjointClasses(ReputationRisk OperationalRisk)

Class(Ressource complete
                restriction(operate someValuesFrom(Activity)))
SubClassOf(Ressource owl:Thing)

Class(Schedule partial Soundness)
DisjointClasses(Schedule Efficiency Effektiveness)
```

```
Class(Security partial Property)
DisjointClasses(Security Soundness Compliance)

Class(Software partial ITComponent)
DisjointClasses(Software Network Infrastructure Hardware)

Class(Soundness partial Property)
DisjointClasses(Soundness Compliance Security)
Class(StrategyRisk partial BusinessRisk)
DisjointClasses(StrategyRisk OperationalRisk)

Class(Technology partial Ressource)
DisjointClasses(Technology Process Human)

Class(TechnologyRisk complete OperationalRisk
             restriction(operatedBy allValuesFrom(Technology)))

Class(Termination partial ITManagementTask)
DisjointClasses(Termination Operation Introduction Migration
                Development)

Class(Timeliness partial Compliance)
DisjointClasses(Timeliness Completeness Correctness)

Class(ValueChain partial owl:Thing
                 restriction(compose someValuesFrom(Activity)))


/////////////////////////////////////////////////////////////
 * Individuals
 /////////////////////////////////////////////////////////////


Individual(agencyService type(BusinessLine))

Individual(assetManagement type(BusinessLine))

Individual(businessDisruptionSystemFailures type(EventType))

Individual(certainty type(Information))

Individual(clientProductsBusinessPractices type(EventType))

Individual(commercialBanking type(BusinessLine))

Individual(corporateFinance type(BusinessLine))

Individual(damagePhysicalAssets type(EventType))

Individual(employmentPracticesWorplaceSafety type(EventType))
```

```
Individual(executionDeliveryProcessManagement type(EventType))
Individual(externalFraud type(EventType))
Individual(internalFraud type(EventType))
Individual(paymentSettlement type(BusinessLine))
Individual(probability type(Information))
Individual(retailBanking type(BusinessLine))
Individual(retailBrokerage type(BusinessLine))
Individual(tradingSales type(BusinessLine))
Individual(uncertainty type(Information))
```

Anhang II
Transformation

```
Namespace(trm = <http://www.jontorisk.org/trm.owl#>)
Namespace(xsd = <http://www.w3.org/2001/XMLSchema#>)
Namespace(rdfs = <http://www.w3.org/2000/01/rdf-schema#>)
Namespace(rdf = <http://www.w3.org/1999/02/22-rdf-syntax-ns#>)
Namespace(owl = <http://www.w3.org/2002/07/owl#>)


Ontology(http://www.jontorisk.org/mview.owl)


/////////////////////////////////////////////////////////////
 * Object Properties
 /////////////////////////////////////////////////////////////


ObjectProperty(exhibitedBy inverseOf(trm:exhibit)
                           domain(trm:Property)
                           range(trm:Ressource))

/////////////////////////////////////////////////////////////
 * Datatype Properties
 /////////////////////////////////////////////////////////////

ObjectProperty(formula Functional
             domain(unionOf(Element Input Output))
             range(<http://www.w3.org/2001/XMLSchema#string>))


/////////////////////////////////////////////////////////////
 * Classes
 /////////////////////////////////////////////////////////////


Class(Asset complete trm:ApplicationSystem)
SubClassOf(Asset owl:Thing)
```

```
Class(Element complete State restriction
            (exhibitedBy allValuesFrom(trm:ApplicationSystem)))

Class(Input complete unionOf
  (restriction(exhibitedBy allValuesFrom(trm:ITComponent))
  restriction(exhibitedBy allValuesFrom(trm:ITManagementTask))))
SubClassOf(Input owl:Thing)

Class(Lossfunction complete trm:Activity)
SubClassOf(Lossfunction owl:Thing)

Class(Output complete trm:Loss restriction
             (trm:generate allValuesFrom(Lossfunction)))

Class(Riskfactor complete unionOf(trm:ITComponent
                                  trm:ITManagementTask))
SubClassOf(Riskfactor owl:Thing)

Class(State complete trm:Property)
SubClassOf(State owl:Thing)
```

Literaturverzeichnis

Abecker, A. und Van Elst, L. (2004): Ontologies for Knowledge Management. In: Staab, S. und Studer, R. (Hrsg.) (2004): Handbook on Ontologies, Springer Verlag, Berlin, S.435-454.

Acerbi, C. und Tasche, D. (2001): Expected Shortfall: A natural coherent alternative to Value at Risk, www.bis.org/bcbs/ca/acertasc.pdf (4.2.2006).

AktG: Aktiengesetz, zuletzt geändert durch Gesetz vom 22.9.2005 (BGBl. I S.2802).

Alavi, M. und Leidner, D. (2001): Review: Knowledge Management and Knowledge Systems: Conceptual Foundations and Research Issues. In: MIS Quarterly, Vol. 25, März 2001, S.107-136.

Albrecht, P. und Maurer, R. (2002): Investment- und Risikomanagement - Modelle, Methoden, Anwendungen, Schäffer-Poeschel Verlag, Stuttgart.

Albrecht, P., Maurer, R. und Mayser, J. (1996): Multi-Faktormodelle: Grundlagen und Einsatz im Management von Aktien-Portefeuilles. In: Zeitschrift für betriebswirtschaftliche Forschung, 1/1996, S.3-27.

Alexander, C. (2003): Statistical models of operational loss. In: Alexander, C. (Hrsg.) (2003): Operational Risk - Regulation, Analysis and Management, Prentice Hall, London, S.129-170.

Allen, L., Boudoukh, J. und Saunders, A. (2004): Understanding Market, Credit, and Operational Risk - The Value at Risk Approach, Blackwell Publishing, Malden (Mass.).

Antoniou, G. und Van Harmelen, F. (2004): Web Ontology Lanuage: OWL. In: Staab, S. und Studer, R. (Hrsg.) (2004): Handbook on Ontologies, Springer Verlag, Berlin, S.67-92.

Artzner, P. et al. (1997): Thinking Coherently. In: Risk Magazine, 10/1997, S.68-72.

Artzner, P. et al. (1999): Coherent Measures of Risk. In: Mathematical Finance, 9/1999, S.203-228.

Baader, F., Horrocks, I. und Sattler, U. (2004): Desciption Logics. In: Staab, S. und Studer, R. (Hrsg.) (2004): Handbook on Ontologies, Springer Verlag, Berlin, S.3-28.

Baetge, J. und Schulze, D. (1998): Möglichkeiten der Objektivierung der Lageberichterstattung über "Risiken der künftigen Entwicklung". In: Der Betrieb, 19/1998, S.937-948.

Bank for International Settlement (BIS 2005): Derivatives statistics - Dezember 2005, http://www.bis.org/statistics/derstats.htm (8.3.2006).

Barth, J. (2000): Worst-Case-Analysen des Ausfallrisikos von Finanzderivaten unter Berücksichtigung von Markteinflüssen, Kovac Verlag, Hamburg.

Basel Committee on Banking Supervision (BCBS 2001): Consultative Document - Operational Risk, www.bis.org/publ/bcbsca07.pdf (4.2.2006).

Basel Committee on Banking Supervision (BCBS 2002): The Quantitative Impact Study for Operational Risk: Overview of Individual Loss Data and Lessons Learned.

Basel Committee on Banking Supervision (BCBS 2003a): Operational risk transfer across financial sectors, http://www.bis.org/publ/joint06.pdf (12.2.2006).

Basel Committee on Banking Supervision (BCBS 2003b): Sound Practices for the Management and Supervision of Operational Risk, http://www.bis.org/publ/bcbs96.pdf (1.10.2005).

Basel Committee on Banking Supervision (BCBS 2003c): The 2002 Loss Data Collection Exercise for Operational Risk: Summary of the Data Collected.

Basel Committee on Banking Supervision (BCBS 2004): Working Paper No. 13: Bank Failures in Mature Economies, http://www.bis.org/publ/ bcbs_wp13.pdf (28.2.2006).

Basel Committee on Banking Supervision (BCBS 2005): Outsourcing in Financial Services, http://www.bis.org/publ/joint12.pdf (7.3.2006).

Basel Committee on Banking Supervision Basel II (Basel II): International Convergence of Capital Measurement and Capital Standards - A revised Framework, Stand: November 2005.

Becker, J. et al. (2004): Wissenschaftstheoretische Grundlagen und ihre Rolle für eine konsensorientierte Informationsmodellierung. In: Frank, U. (Hrsg.) (2004): Wissenschaftstheorie in Ökonomie und Wirtschaftsinformatik, Deutscher Universitäts-Verlag, Wiesbaden, S.335-366.

Berger, H. (1980): Schadensverteilung bei Bankbetriebsstörungen, Haag und Herchen Verlag, Frankfurt (Main).

Berners-Lee, T., Hendler, J. und Lassila, O. (2001): The Semantic Web. In: Scientific American, Vol. 284, Mai 2001, S.34-44.

Bessis, J. (2002): Risk Management in Banking, Wiley, Chichester.

Bestmann, U. et al. (1997): Kompendium der Betriebswirtschaftslehre, Oldenbourg Verlag, München.

Beyer, O. et al. (1980): Wahrscheinlichkeitsrechnung und mathematische Statistik, Deutsch Verlag, Frankfurt (Main).

BGB: Bürgerliches Gesetzbuch, zuletzt geändert durch Gesetz vom 7. Juli 2005 (BGBl. I S.1970).

Bhattacharya, S., Boot, A. W. A. und Thakor, A.V. (1998): The Economics of Bank Regulation. In: Journal of Money, Credit, and Banking, Vol. 30, S.745-770.

Biermann, B. (2002): Modernes Risikomanagement in Banken. In: Eller, R., Gruber, W. und Reif, M. (Hrsg.) (2002): Handbuch des Risikomanagements, Schäffer-Poeschel Verlag, Stuttgart, S.103-125.

Bomsdorf, E. (1995): Induktive Statistik - Eine Einführung, Josef Eul Verlag, Bergisch Gladbach.

Börner, C. (2004): Kernkompetenz Kundennähe. Grenzen der Bank: Wertschöpfungsparter oder Vertriebsstelle?. In: GENO - Zeitschrift des Württembergischen Genossenschaftsverbandes, 9, S.4-8.

Braun, H. (1984): Risikomanagement: eine spezifische Controllingaufgabe, S.Toeche-Mittler Verlag, Darmstadt.

Bundesamt für Sicherheit in der Informationstechnik (BSI 2005): Leitfaden IT-Sicherheit, http://www.bsi.de/gshb/Leitfaden/GS-Leitfaden.pdf (01.10.2005).

Bundesamt für Sicherheit in der Informationstechnik ITGS (BSI ITGS): IT-Grundschutzhandbuch, Stand: November 2004.

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin 2005a): Anlage 1: (Erläuterungen MaRisk) zum Rundschreiben 18/2005, http://www.bafin.de/rundschreiben/89_2005/051220_anl1.pdf (8.3.2006).

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin 2005b): Anschreiben zum Rundschreiben 18/2005 Veröffentlichung der Endfassung MaRisk, http://www.bafin.de/schreiben/89_2005/051220.htm (8.3.2006).

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin 2006): Aufgaben und Ziele der Bankenaufsicht, www.bafin.de (28.2.2006).

Bundesanstalt für Finanzdienstleistungsaufsicht MaRisk (MaRisk): Mindestanforderungen an das Risikomanagement, Stand: 20.12.2005.

Cap Gemini Ernst & Young (2002): Operationelle Risiken bei Kreditinstituten - Trends & Best Practice.

Chong, Y. (2004): Investment Risk Management, Wiley, Chichester.

Coleman, R. (2000): Using Modelling in Operational Risk Management, http://stats.ma.imperial.ac.uk/rcoleman/public_html/iir.pdf (21.11.2005).

Commerzbank (2004): Commerzbank Geschäftsbericht 2004.

Committee of European Insurance and Occupational Pensions Supervisors (CEIOPS 2006): Consultation on Solvency II, http://www.ceiops.org/ (8.3.2006).

Cormen, T. H., Leiserson, C. E. und Rivest, R. L. (1998): Introduction to Algorithms, MIT Press, Cambridge (Mass).

Cruz, M. G. (2002): Modeling, measuring and hedging operational risk, Wiley, Chichester.

Culp, C. (2002): The art of Risk management - Alternative Risk Transfer, Capital Structure, and the convergence of Insurance and Capital Markets, Wiley, Chichester.

Cummins, D., Lewis, C. und Wei, R. (2004): The Market Value Impact of Operational Risk Events For U.S. Banks and Insurers, http://ssrn.com/abstract=640061 (12.2.2006).

Cuske, C. et al. (2007): Resolving Conceptual Ambiguities in Technology Risk Management, noch nicht erschienen, voraussichtlich: 2007.

Cuske, C., Dickopp, T. und Schader, M. (2005): Konzeption einer Ontologie-basierten Quantifizierung operationeller Technologierisiken bei Banken. In: Sonderheft zur Multi-Konferenz Wirtschaftsinformatik 2006, 4/2005, S.61-74.

Cuske, C., Dickopp, T. und Seedorf, S. (2005): An Ontology-based Platform for Knowledge-based Simulation Modeling in Financial Risk Management. In Proceedings: The 2005 European Simulation and Modelling Conference, 24.-26. Oktober 2005, Porto, Portugal.

Danielsson, J. et al. (2001): An Academic Response to Basel II, http://www.cermas.gsu.edu/Documents/embrechts.pdf (4.2.2006).

Davenport, T. und Prusak, L. (1998): Working Knowledge: How Organizations Manage What They Know, Harvard Business School, Boston.

Deutsche Bank (2004): Deutsche Bank Finanzbericht 2004.

Deutsche Bundesbank (2005): Monatsbericht September 2005.

Deutsche Bundesbank und BaFin (2005): Bericht über die Industrieaktion AMA operationelles Risiko, www.bundesbank.de/download/bankenaufsicht/pdf/ama/abschlussbericht.pdf (1.12.2005).

Diggelmann, P. (1999): Value at risk - kritische Betrachtung des Konzepts; Möglichkeiten der Übertragung auf den Nichtfinanzbereich, Versus Verlag, Zürich.

Dötz, N. (2002): Bankenregulierung - regelgebunden oder diskretionär?, Josef Eul Verlag, Lohmar.

Dowd, V. (2003): Measurement of Operational Risk: the Basel Approach. In: Alexander, C. (Hrsg.) (2003): Operational Risk - Regulation, Analysis and Management, Prentice Hall, London, S.31-48.

Dresdner Bank (2004): Dresdner-Bank-Konzern Finanzbericht 2004.

Ebnöther, S. et al. (2002): Operational Risk: A Practitioner's view, http://www.gloriamundi.org/download.asp?ResouceUrl=pamavpes.pdf (20.12.2005).

Eisenführ, F. und Weber, M. (2003): Rationales Entscheiden, Springer Verlag, Berlin.

Embrechts, P., Furrer, H. und Kaufmann, R. (2003): Quantifying regulatory capital for operational risk, http://www.math.ethz.ch/~baltes/ftp/OPRiskWeb.pdf (5.11.2005).

Embrechts, P., Klüppelberg, C. und Mikosch, T. (1997): Modelling Extremal Events for Insurance and Finance, Springer Verlag, Berlin.

EU (1999): Überarbeitung der Eigenkapitalvorschriften für Kreditinstitute und Wertpapierfirmen in der EU - Konsultationspapier, http://europa.eu.int/comm/internal_market/en/finances/banks/capadde.pdf (8.3.2006).

European Central Bank (ECB 2004): Report on EU Banking Structure - November 2004.

European Central Bank (ECB 2005a): EU Banking Sector Stability - October 2005.

European Central Bank (ECB 2005b): Occasional Paper Series No. 42, http://www.ecb.int/pub/pdf/scpops/ecbocp42.pdf (8.3.2006).

European Comission CAD III (CAD III) (CAD III): Capital Adequacy Directive, Stand: 14. Juli 2004.

Fachgruppe Modellierung betrieblicher Informationssysteme (Mobis 2006): Mobis Portal, http://www.wi-inf.uni-essen.de/MobisPortal/ (8.3.2006).

Faisst, U. (2004): Ein Modell zur Steuerung operationeller Risiken in IT-gestützten Bankprozessen. In Proceedings: Multikonferenz Wirtschaftinformatik 2004, 09.-11. März 2004, Essen, Deutschland.

Faisst, U. und Kovacs, M. (2003): Quantifizierung operationeller Risiken - ein Methodenvergleich. In: Die Bank, 5/2003, S.342-349.

Farny, D. (1979): Grundfragen des Risk Management. In: Goetzke, W. und Sieben, G. (Hrsg.) (1979): Risk-Management, Strategien zur Risikobeherrschung, GEBERA Verlag, Köln, S.11-37.

Fasse, F.-W. (1995): Risk-Management im strategischen internationalen Marketing, S+W Steuer- und Wirtschaftsverlag, Hamburg.

Federal Reserve System (Fed 2005): Results of the 2004 Loss Data Collection Exercise for Operational Risk.

Fensel, D. (2004): Ontologies: A Silver Bullet for Knowledge Management and Electronic Commerce, Springer Verlag, Berlin.

Fernandez-Lopez, M., Gomez-Perez, A. und Juristo, N. (1997): METHONTOLOGY: From Ontological Art Towards Ontological Engineering. In Proceedings: 1997 AAAI Spring Symposium on Ontological Engineering, 24.-26. März 1997, Stanford, Kalifornien, USA.

Fisher, R. und Tippett, L. H. C. (1928): Limiting forms of the frequency distribution of largest or smallest member of a sample. In: Cambridge Philosophical Society, 24, S.180-190.

Fishwick, P. A. (1995): Simulation Model Design and Execution: Building Digital Worlds, Prentice Hall, Englewood Cliffs.

Fishwick, P. A. und Miller, J. A. (2004): Ontologies for Modeling and Simulation: Issues and Approaches. In Proceedings: The 2004 Winter Simulation Conference, 5.-8. Dezember 2004, Washington, D.C., USA.

Fitch (2004): Operational Risk Management & Basel II Implementation: Survey Results.

Foit, M. (2005): Management operationeller IT-Risiken in Banken - Rechtliche und steuerliche Aspekte der Bewertung operationeller Risiken von IT- und Outsourcing-Projekten, Universitätsverlag Regensburg, Regensburg.

Fontnouvelle, P. et al. (2003): Using Loss Data to quantify Operational Risk, http://ssrn.com/abstract=395083 (21.1.2006).

Fontnouvelle, P. und Rosengren, E. (2004): Implications of Alternative Operational Risk Modeling Techniques, http://ssrn.com/abstract=663485 (21.1.2006).

Frachot, A., Georges, P. und Roncalli, T. (2001): Loss Distribution Approach for operational risk, http://gro.creditlyonnais.fr/content/wp/lda.pdf (21.1.2006).

Fürer, G. (1990): Risk Management im internationalen Bankgeschäft, Paul Haupt Verlag, Bern.

Füser, K., Rödel, K. und Kang, D. (2002): Identifizierung und Quantifizierung von "Operational Risk". In: Finanz Betrieb, 9/2002, S.495-502.

Gammelin, K. und Buchhart, A. (2004): Die Praxis des Risikomanagements in Finanzdienstleistungsunternehmen. In: Finanz Betrieb, 3/2004, S.178-184.

Garrido, J. (2001): Object-Oriented Discrete-Event Simulation with Java, Kluwer Academic, New York.

Gaulke, M. (2002): Risikomanagement in IT-Projekten, Oldenbourg Verlag, München.

GO30 (1993): Special Report on Global Derivatives - Derivatives: Practices & Principles, http://www.group30.org/pubs.php?page=pubs1993.html (8.3.2006).

Gomez-Perez, A., Fernandez-Lopez, M. und Corcho, O. (2004): Ontological engineering: with examples from the areas of knowledge management, e-commerce and the semantic web, Springer Verlag, London.

Grauman, M. (2003): Controlling - Begriff, Elemente, Methoden und Schnittstellen, IDW Verlag, Düsseldorf.

Gruber, T. (1995): Toward Principles for the Design of Ontologies Used for Knowledge Sharing. In: International Journal Human and Computer Studies, 43(5/6), S.907-928.

Gruber, W. (2001): Konzepte zur Messung von Markt- und Kreditrisiken. In: Eller, R., Gruber, W. und Reif, M. (Hrsg.) (2001): Handbuch Gesamtbanksteuerung, Schäffer-Poeschel Verlag, Stuttgart, S.80-101.

Grüninger, M. und Fox, M. (1995): Methodology for the design and evaluation of ontologies. In Proceedings: IJCAI-95, Workshop on Basic Ontological Issues in Knowledge Sharing, 20.-25. August 1995, Montreal, Kanada.

Guarino, N. (1998): Formal Ontology and Information Systems. In Proceedings: FOIS'98, 6.-8. Juni 1998, Trento, Italien.

Guarino, N. und Persidis, A. (2003): Deliverable 3.5 Evaluation Framework for Content Standards, http://ontoweb.aifb.uni-karlsruhe.de/Members/ruben/Deliverable%203.5 (21.11.2005).

Guthoff, A., Pfingsten, A. und Wolf, J. (1998): Der Einfluss einer Begrenzung des Value at Risk oder des Lower Partial Moment One auf die Risikoübernahme. In: Ohler, A. (Hrsg.) (1998): Credit Risk und Value-at-Risk Alternativen, Schäffer-Poeschel Verlag, Stuttgart, S.111-153.

Haaß, J. (2001): Die Informations- und Risikoabbildung von Banken nach Handels- und Aufsichtsrecht, Dissertation, Universität Karlsruhe, Karlsruhe.

Hammer, S. (1999): Die 2. Dimension der IT-Sicherheit: verletzlichkeitsreduzierende Technikgestaltung am Beispiel von Public-key-Infrastrukturen, Vieweg Verlag, Wiesbaden.

Hartmann-Wendels, T., Pfingsten, A. und Weber, M. (2004): Bankbetriebslehre, Springer Verlag, Berlin.

Haubenstock, M. und Hardin, L. (2003): The Loss Distribution Approach. In: Alexander, C. (Hrsg.) (2003): Operational Risk - Regulation, Analysis and Management, Prentice Hall, London, S.171-192.

Heinen, E. (1966): Das Zielsystem der Unternehmung - Grundlagen betriebswirtschaftlicher Entscheidungen, Gabler Verlag, Wiesbaden.

Hesse, C. (2003): Angewandte Wahrscheinlichkeitstheorie, Vieweg Verlag, Braunschweig.

Horn, C. und Müller, C. (2001): Operational Risk Management - Anmerkungen zu Begriff, Methoden und Implementierung. In: Zeitschrift für das gesamte Kreditwesen, 4/2001, S.194-199.

HP Labs Semantic Web Research (2005): Jena - A Semantic Web Framework for Java, http://jena.sourceforge.net/ (8.3.2006).

Hypovereinsbank (2004): HVB Group Geschäftsbericht 2004.

ibi research (2004): Risikomanagement in der Finanzwirtschaft und Industrie - Eine Analyse des Managements operationeller Risiken in deutschen Industrie- und Dienstleistungsunternehmen.

Imboden, C. (1983): Risikohandhabung: Ein entscheidungsbezogenes Verfahren, Paul Haupt Verlag, Bern.

Institut der Wirtschaftsprüfer Prüfungsstandard 330 (IDW PS 330): Abschlußprüfung bei Einsatz von Informationstechnologie, Stand: 24.09.2002.

Institut der Wirtschaftsprüfer Prüfungsstandard 340 (IDW PS 340): Die Prüfung des Risikofrüherkennungssystems nach § 317 Abs. 4 HGB, Stand: 1999.

Institut der Wirtschaftsprüfer Stellungnahme zur Rechnungslegung FAIT 1 (IDW RS FAIT 1): Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie, Stand: 24.09.2002.

IT Governance Institute (2003): Board Briefing on IT Governance, http://www.isaca.org/Content/ContentGroups/ITGI3/Resources1/Board_Briefing_on_IT_Governance/26904_Board_Briefing_final.pdf (26.2.2006).

IT Governance Institute COBIT (ITGI COBIT): Control Objectives for Information and Related Technology, Stand: Juli 2002.

Jacobs, T. A. (2004): Risk Models and Basel II: A Review of the Literature, http://www.business.uiuc.edu/c-kahn/Fin427/ThomasJacobs_Review.pdf (21.1.2006).

Jeffery, C. (2005): Operational Risk - Falling short of the mark. In: Risk Magazine, 9/2005, S.91-93.

Jörg, M. (2002): Operational Risk - Herausforderungen bei der Implementierung von Basel II, Bankakdamie Verlag, Frankfurt (Main).

Junginger, M., von Balduin, A. und Krcmar, H. (2003): Operational Value at Risk und Management von IT-Risiken. In: WISU, 03/2003, S.356-364.

Karl, D. B. (1996): Eiffizienz ist eine Frage der Architektur. In: Bank Magazin, 8/1996, S.8-10.

Kemper, A. und Eickler, A. (1999): Datenbanksysteme - Eine Einführung, Oldenbourg Verlag, München.

King, J. L. (2001): Operational Risk: measurement and modelling, Wiley, Chichester.

Knight, F. (1965): Risk, Uncertainty and Profit, Harper & Row (Reprint 1921), New York.

Knuth, D. E. (1998): The art of computer programming, volume 2: Seminumerical algorithms, Addison-Wesley, Reading (Mass).

Krcmar, H. (2005): Informationsmanagement, Springer Verlag, Berlin.

Krümmel, H. J. (1989): Unternehmenspolitische Vorgaben für die Risikosteuerung der Bank. In: Krümmel und Rudolph (Hrsg.) (1989): Finanzintermediation und Risikomanagement - Vorträge und Berichte der Tagung Finanzintermediation und Risikomanagement am 15. September 1989, Knapp Verlag, Frankfurt (Main), S.32-56.

Krystek, U. und Müller, M. (1999): Frühaufklärungssysteme - Spezielle Informationssysteme zur Erfüllung der Risikokontrollpflicht nach KonTraG. In: Controlling, 4/5/1999, S.177-182.

Kühn, R. und Neu, P. (2003): Functional correlation approach to operational risk in banking organizations. In: Physica A: Statistical Mechanics and its Applications, 322, S.650-666.

Kühn, R. und Neu, P. (2004): Adequate Capital and Stress Testing for Operational Risks, http://www.mth.kcl.ac.uk/~kuehn/published/OR_RiskWaters2.pdf (21.1.2006).

Kupsch, P. (1973): Das Risiko im Entscheidungsprozess, Gabler Verlag, Wiesbaden.

KWG: Gesetz über das Kreditwesen (Kreditwesengesetz - KWG), zuletzt geändert durch Gesetz vom 22. September 2005 (BGBl. I S.2809).

L'Ecuyer, P. (2001): Software for Uniform Random Number Generation: Distinguishing the good and the bad. In Proceedings: The 2001 Winter Simulation Conference, 9.-12. Dezember 2001, Arlington, Virginia, USA.

L'Ecuyer, P. (2005): SSJ User's Guide Package rng - Random Number Generators, http://www.iro.umontreal.ca/~simardr/ssj/doc/pdf/guiderng.pdf (8.3.2006).

L'Ecuyer, P. (2006): SSJ: Stochastic Simulation in Java, http://www.iro.umontreal.ca/~simardr/ssj/ (8.3.2006).

Lacy, L. und Gerber, W. (2004): Potential modeling and simulation applications of the web ontology language - OWL. In Proceedings: The 2004 Winter Simulation Conference, 5.-8. Dezember 2004, Washington D.C., USA.

Lamberti, H.-J. (2004): Industrialisierung des Bankgeschäfts. In: Die Bank, 6-7/2004, S.370-375.

Leemis, L. (1996): Discrete-Event Simulation Input Process Modeling. In Proceedings: The 1996 Winter Simulation Conference, 8.-11. Dezember 1996, Coronado, Kalifornien, USA.

Leippold, M. und Vanini, P. (2003): The Quantification of Operational Risk, http://ssrn.com/abstract=481742 (21.1.2006).

Leippold, M. und Vanini, P. (2005): The Quantification of Operational Risk. In: Journal of Risk, 8/1, S.59-85.

Leippold, M., Doebli, B. und Vanini, P. (2003): From Operational Risk to Operational Excellence, http://ssrn.com/abstract=413720 (22.1.2006).

Liekweg, A. (2003): Risikomanagement und Rationalität: Präskriptive Theorie und praktische Ausgestaltung von Risikomanagement, Deutscher Universitäts-Verlag, Wiesbaden.

Locher, C., Mehlau, J. und Wild, O. (2004): Towards Risk Adjusted Controlling of Strategic IS Projects in Banks in the Light of Basel II. In Proceedings: The 37th Hawaii International Conference on System Sciences 2004, 5.-8. Januar 2004, Big Island, Hawaii, USA.

Lubich, R. und Aumer, T. (2003): Outsourcing im WP-Service: Die Total Cost of Ownership sind entscheidend. In: Kipker, I. und Veil, M. (Hrsg.) (2003): Transaction Banking - Strategien, Organisation, Steuerungsinstrumente, Gabler Verlag, Wiesbaden, S.47-59.

Lück, W. (1998): Elemente eines Risiko-Managements. In: Der Betrieb, 1/2 1998, S.8-15.

Mag, W. (1977): Entscheidung und Information, Vahlen Verlag, München.

Marshall, C., Prusak, L. und Shpilberg, D. (1996): Financial Risk and the Need for Superior Knowledge Management. In: California Management Review, 38/3, S.77-101.

Martin, T. und Bär, T. (2002): Grundzüge des Risikomanagements nach KonTraG: das Risikomanagementsystem zur Krisenfrüherkennung nach § 91 Abs. 2 AktG, Oldenbourg Verlag, München.

Matsumoto, M. und Nishimura, T. (1998): Mersenne Twister: A 623-dimensionally equidistributed uniform pseudo-random number generator. In: ACM Transactions on Modeling and Computer Simulation, 8/1998, S.3-30.

McBride, B. (2004): The Resource Description Framework (RDF) and its Vocabulary Description Language (RDFS). In: Staab, S. und Studer, R. (Hrsg.) (2004): Handbook on Ontologies, Springer Verlag, Berlin, S.51-66.

McNeil, A. (2000): Extreme Value Theory for Risk Managers. In: Embrechts, P. (Hrsg.) (2000): Extremes and Integrated Risk Management, Risk Books, London, S.3-18.

McNeil, A. J. und Saladin, T. (1997): The Peaks over Thresholds Method for Estimating High Quantiles of Loss Distributions, http://www.math.ethz.ch/~mcneil/ftp/cairns.pdf (22.1.2006).

McNeil, A. J., Frey, R. und Embrechts, P. (2006): Quantitative Risk Management: Concepts, Techniques and Tools, noch nicht erschienen, voraussichtlich: 2006.

Mensch, G. (1991): Risiko und Unternehmensführung: eine systemorientierte Konzeption zum Risikomanagement, Peter Lang Verlag, Frankfurt (Main).

Miller, J. A. et al. (2004): Investigating Ontologies for Simulation Modeling. In Proceedings: 37th Annual Simulation Symposium (ANSS'04), 18.-22. April 2004, Arlington, Virgina, USA.

Miller, J. A. et al. (2006): Ontologies for Modeling and Simulation: An Extensible Framework, noch nicht erschienen, voraussichtlich: 2006.

Minz, K.-A. (2004): Operationelle Risiken in Kreditinstituten, Bankakademie Verlag, Frankfurt (Main).

Moormann, J. und Möbus, D. (2004): Wertschöpfungsmanagement in Banken, Bankakademie Verlag, Frankfurt (Main).

Morgenstern, U. (2004): Interne Modelle in der aufsichtsrechtlichen Risikomessung des Eigenhandelsgeschäftes mittelgroßer Kreditinstitute: Vorteilhaftigkeitsvergleich der Eigenmittelunterlegung der Marktrisikoposition, Knapp Verlag, Frankfurt (Main).

Moscadelli, M. (2004): The Modelling of Operational Risk: Experience with the Analysis of the Data Collected by the Basel Committee, http://ssrn.com/abstract=557214 (22.1.2006).

Münchbach, D. (2001): Management der operationellen Risiken des Private Banking, Difo-Druck, Bern.

Musa, J. D., Iannino, A. und Okumoto, K. (1987): Software Reliability - Measurement, Prediction, Application, McGraw-Hill, New York.

Nance, R. E. (1993): A History of Discrete Event Simulation Programming Languages. In Proceedings: History of Programming Languages Conference, 20.-23. April 1993, Cambridge, Massachusetts, USA.

Neubeck, G. (2003): Prüfung von Risikomanagementsystemen, IDW Verlag, Düsseldorf.

Nonaka, I. (1994): A Dynamic Theory of Organizational Knowledge Creation. In: Organization Science, Februar 1994, S.14-37.

Nowack, A. (1994): Prognose bei unregelmäßigem Bedarf. In: Mertens, P. (Hrsg.) (1994): Prognoserechnung, Physica Verlag, Heidelberg, S.57-68.

Noy, N. und Musen, M. (2004): Specifying Ontology Views by Traversal. In Proceedings: Third International Semantic Web Conference, 7.-11. November 2004, Hiroshima, Japan.

Oehler, A. und Unser, M. (2001): Finanzwirtschaftliches Risikomanagement, Springer Verlag, Berlin.

Peuker, J. (1994): Grundlagen der Datenverarbeitung, Schmidt Verlag, Gießen.

Pezier, J. (2003): A constructive review of the Basel proposals on operational risk. In: Alexander, C. (Hrsg.) (2003): Operational Risk - Regulation, Analysis and Management, Prentice Hall, London, S.49-73.

Pham, H. (2000): Software reliability, Springer Verlag, New York.

Piaz, J.-M. (2002): Operational Risk Management bei Banken, Versus Verlag, Zürich.

Picoult, E. (1999): Calculating Value-at-Risk with Monte Carlo Simulation. In: Risk Books (Hrsg.) (1999): Internal Modelling and CAD II - Qualifying and Quantifying Risk within a Financial Institution, BA, British Bankers' Association, London, S.73-92.

Poddig, T. und Kunze, B. (2003): Risikomanagementsysteme bei Banken vor dem Hintergrund der staatlichen Regulierung des Finanzsektors. In: Finanz Betrieb, 11/2003, S.693-702.

Porter, M. E. (2000): Wettbewerbsvorteile - Spitzenleistungen erreichen und behaupten, Campus Verlag, Frankfurt.

Postbank (2004): Postbank Konzern Geschäftsbericht 2004.

Probst, C. (2003): Referenzmodell für IT-Service-Informationssysteme, Logos Verlag, Berlin.

R Development Core Team (2005): R: A language and environment for statistical computing, http://cran.r-project.org/ (8.3.2006).

Rachev, S., Chernobai, A. und Menn, C. (2004): Empirical Examination of Operational Loss Distribution, http://www.statistik.uni-karlsruhe.de/technical_reports/festschrift_ed.pdf (12.2.2006).

Read, O. (1998): Parametrische Modelle zur Ermittlung des Value-at-Risk, Dissertation, Universität Köln, Köln.

Rmetrics (2006): Option Valuation, http://cran.r-project.org/src/contrib/Descriptions/fOptions.html (8.3.2006).

Röckle, S. (2002): Schadensdatenbanken als Instrument zur Quantifizierung von Operational Risk in Kreditinstituten, Verlag Wissenschaft & Praxis, Sternenfels.

Rode, M. und Moser, C. (1999): Die neuen Basler Eigenkapitalanforderungen. In: Zeitschrift für das gesamte Kreditwesen, 14/1999, S.720-724.

RoSuDa (2005): Java/R Interface (JRI), http://rosuda.org/software/JRI/ (8.3.2006).

Rünger, P. und Walther, U. (2004): Die Behandlung der operationellen Risiken nach Basel II - ein Anreiz zur Verbesserung des Risikomanagements?, http://www.uni-freiberg.de/~wwwfak6/paper/walther_14_2004.pdf (4.2.2006).

Sampson, G. (2004): Reassessing self-assessment. In: Risk Magazine, August 2004, S.71-75.

Sandmann, K. (1999): Einführung in die Stochastik der Finanzmärkte, Springer Verlag, Heidelberg.

Schäl, I. und Stummer, W. (2005): Kategorisierung operationeller Risiken im Umfeld von Basel II. In: Finanz Betrieb, 12/2005, S.786-798.

Scharpf, P. und Luz, G. (2000): Risikomanagement, Bilanzierung und Aufsicht von Finanzderivaten, Schäffer-Poeschel Verlag, Stuttgart.

Schierenbeck, H. (2003): Ertragsorientiertes Bankmanagement. Band 2: Risiko-Controlling und integrierte Rendite-/Risikosteuerung, Gabler Verlag, Wiesbaden.

Schmidt, J. W. (1984): Introduction to Simulation. In Proceedings: The 1984 Winter Simulation Conference, 28.-30. November 1984, Dallas, USA.

Schneider, A. (2005): Risikomanagement ist Trumpf: Die Entwicklung der Mindestanforderungen an das Risikomanagement (MaRisk). In: Becker, A. und Wolf, M. (Hrsg.) (2005): Prüfungen in Kreditinstituten und Finanzdienstleistungsunternehmen, Schäffer-Poeschel Verlag, Stuttgart, S.577-594.

Schuy, A. (1989): Risiko-Management: eine theoretische Analyse zum Risiko und Risikowirkungsprozess als Grundlage für ein risikoorientiertes Management unter besonderer Berücksichtigung des Marketing, Peter Lang Verlag, Frankfurt (Main).

Singpurwalla, N. und Wilson, S. (1999): Statistical methods in software engineering: reliability and risk, Springer Verlag, New York.

Sitt, A. (2003): Dynamisches Risiko-Management: zum unternehmerischen Umgang mit Risiken, Deutscher Universitäts-Verlag, Wiesbaden.

Smithson, C. und Song, P. (2004): Quantifying operational risk. In: Risk Magazine, 07/2004, S.57-59.

Snyder, C. und Wilson, L. (1998): The Process of Knowledge Harvesting: The Key to Knowledge Management. In Proceedings: Business Information Management - BIT Conference 98, November 1998, Manchester, UK.

Spahr, R. (2001): Steuerung operationaler Risiken im Electronic und Investment Banking. In: Die Bank, 9/2001, S.660-663.

Spellmann, F. (2002): Gesamtrisiko-Messung von Banken und Unternehmen, Deutscher Universitäts-Verlag, Wiesbaden.

Stahlknecht, P. und Hasenkamp, U. (1997): Einführung in die Wirtschafts-informatik, Springer Verlag, Berlin.

Stanford Medical Informatics (2005): Protege, http://protege.stanford.edu/ (8.3.2006).

Straßberger, M. (2002): Risikokapitalallokation und Marktpreisrisikosteuerung mit Value-at-Risk-Limiten, Josef Eul Verlag, Lohmar.

Studer, G. (1998): VaR als Risiko. In: Schweizer Bank, 9/1998, S.54-56.

Süchting, J. und Paul, S. (1998): Bankmanagement, Schäffer-Poeschel Verlag, Stuttgart.

Tabbert, C. (2003): Zukunftsfähigkeit von Bank-Software-Architekturen, Universitätsverlag Regensburg, Regensburg.

Uschold, M. und Grüninger, M. (1996): Ontologies: Principles, Methods and Applications. In: Knowledge Engineering Review, 2/1996, S.93-136.

Uschold,M. (1998): The Enterprise Ontology. In: Knowledge Engineering Review, 13(1)/1998, S.31-89.

Utz, E. (2002): Bedeutung operationeller Risiken aus Sicht von Banken und Sparkassen. In: Eller, R., Gruber, W. und Reif, M. (Hrsg.) (2002): Handbuch operationelle Risiken, Schäffer-Poeschel Verlag, Stuttgart, S.97-123.

Van den Brink, G. J. (2001): Operational Risk - Wie Banken das Betriebsrisiko beherrschen, Schäffer-Poeschel Verlag, Stuttgart.

Van den Brink, G. J. (2003): Quantifizierung operationeller Risiken - Ein Weg zur Einbettung in den Management-Zyklus. In: RiskNEWS, Januar/Februar 2003, S.26-36.

Versteegen, G. (2003): Risikomanagement in IT-Projekten: Gefahren rechtzeitig erkennen und meistern, Springer Verlag, Berlin.

Vögtle, M. (1997): Intelligente Informationssysteme für das Bankgeschäft: eine theoretische und empirische Analyse ihrer strategischen Bedeutung, Haufe Verlag, Freiburg.

Volck, S. (1997): Die Wertkette im prozessorientierten Controlling, Deutscher Universitäts-Verlag, Wiesbaden.

Volz, R., Oberle, D. und Studer, R. (2003): Views for light-weight web ontologies. In Proceedings: The 2003 ACM Symposium on Applied Computing, 9.-12. März 2003, Melbourne, Florida, USA.

W3C (2004a): OWL Web Ontology Language - Semantics and Abstract Syntax, http://www.w3.org/2004/OWL/ (8.3.2006).

W3C (2004b): RDF Vocabulary Description Language 1.0: RDF Schema - W3C Recommendation 10 February 2004, http://www.w3.org/TR/rdf-schema/ (8.3.2006).

W3C (2004c): Resource Description Framework (RDF), http://www.w3.org/RDF/ (8.3.2006).

W3C (2006): SPARQL Query Language for RDF - W3C Working Draft 20. Februar 2006, http://www.w3.org/TR/rdf-sparql-query/ (8.3.2006).

Wade, M. und Hulland, J. (2004): Rewiew: The Resource-based View and Information Systems Research: Review, Extension, and Suggestions for Future Research. In: MIS Quarterly, Vol.28, März 2004, S.107-142.

Wallmeier, M. (1997): Prognose von Aktienrenditen und -risiken mit Mehrfaktorenmodellen, Uhlenbruch Verlag, Bad Soden (Taunus).

Wand, M. P. und Jones, M. C. (1995): Kernel Smoothing, Chapman & Hall, London.

Wand, M. und Ripley, B. (2005): The KernSmooth Package, http://www.maths.unsw.edu.au/~wand (8.3.2006).

Weber, K. (2004): Der wissenschaftstheoretische Status von Simulationen. In: Frank, U. (Hrsg.) (2004): Wissenschaftstheorie in Ökonomie und Wirtschaftsinformatik, Deutscher Universitäts-Verlag, Wiesbaden, S.191-210.

Welty, C. und Guarino, N. (2001): Supporting ontological analysis of taxonomic relationships. In: Data & Knowledge Engineering, 39(1), S.51-74.

Wills, S. (1999): Rewards on offer from a new discipline. In: Risk Magazine, 11/1999, S.52-54.

Wolf, E. (2005): IS Risks and Operational Risk Management in Banks, Josef Eul Verlag, Lohmar.

Wolf, K. (2003): Risikomanagement im Kontext der wertorientierten Unternehmensführung, Deutscher Universitäts-Verlag, Wiesbaden.

Wolf, K. und Runzheimer, B. (2003): Risikomanagement und KonTraG: Konzeption und Implementierung, Gabler Verlag, Wiesbaden.

Zeigler, B., Praehofer, H. und Kim, T. G. (2000): Theory of modeling and simulation: integrating discrete event and continuous complex dynamic systems, Academic Press, San Diego.